



U.S. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD
(PCLOB)

PUBLIC FORUM ON FOREIGN INTELLIGENCE SURVEILLANCE ACT
(FISA) SECTION 702

Thursday, January 12, 2023

A P P E A R A N C E S

1

2

3 SHARON BRADFORD FRANKLIN

4 Chair, Privacy and Civil Liberties Oversight Board

5

6 GENERAL PAUL M. NAKASONE

7 United States Army

8 Commander, United States Cyber Command

9 Director, National Security Agency/Chief, Central

10 Security Service

11

12 JULIAN SANCHEZ

13 Cato Senior Fellow

14

15 JERAMIE SCOTT

16 Senior Counsel, Electronic Privacy Information Center

17

18 APRIL DOSS

19 NSA General Counsel

20

21 CHRISTOPHER FONZONE

22 ODNI General Counsel

1

2 CINDY COHN

3 Executive Director, Electronic Frontier Foundation

4

5 MIKE HERRINGTON

6 Senior Operations Advisor, FBI

7

8 DR. JEFF KOSSEFF

9 U.S. Naval Academy

10

11 DR. JONATHAN MAYER

12 Princeton University

13

14

15

16

17

18

19

20

21

22

1 P R O C E E D I N G S

2 MS. FRANKLIN: Hello, I'm Sharon Bradford
3 Franklin, Chair of the Privacy and Civil Liberties
4 Oversight Board. Together with my fellow Board
5 members, Ed Felten, Beth Williams, Travis LeBlanc and
6 Richard DiZinno, I'd like to welcome you to today's
7 public forum.

8 Today's forum will help to inform the Board's
9 oversight of Foreign Intelligence Surveillance Act,
10 Section 702. Section 702 authorizes the government to
11 target non-Americans located outside the United
12 States, and to collect the content of their
13 communications such as e-mail and phone calls. The
14 government may also collect the information of U.S.
15 persons through what is called incidental collection
16 when they are in communication with these foreign
17 targets.

18 Our role as the Privacy and Civil Liberties
19 Oversight Board is to review federal counterterrorism
20 programs to ensure that they include appropriate
21 safeguards for privacy and civil liberties. Since
22 Section 702 is a program with multiple purposes that

1 include counterterrorism, the PCLOB has long conducted
2 oversight of Section 702 surveillance. In fact,
3 dating back to 2014, the PCLOB conducted its first
4 review of surveillance conducted under Section 702 and
5 issued a comprehensive report on Section 702. Indeed,
6 that report is still considered the most comprehensive
7 unclassified description of the Section 702 program.

8 In its report, the Board found that the
9 Section 702 program was valuable, but also identified
10 certain aspects of that program that raise particular
11 privacy risks, including the potentially large scope
12 of incidental collection of U.S. persons'
13 communications, the use of about collection to acquire
14 communications that are neither to nor from targets of
15 surveillance, and the use of queries to search for the
16 communications of specific U.S. persons within the
17 information that has been collected.

18 That report set out 12 recommendations to
19 resolve these issues, most of which have been
20 implemented by the intelligence community, but a
21 number of which have not yet been incorporated into
22 the law and the program's procedures. As people

1 watching this program, that are public forum are
2 likely aware, Section 702 is scheduled to sunset at
3 the end of 2023 unless Congress Acts to reauthorize
4 the statute. To carry out our oversight role, the
5 Board plans to release a new report on Section 702 to
6 inform the upcoming public and congressional debate.

7 This new report will update the PCLOB's 2014
8 report and provide additional recommendations in light
9 of new developments over the past several years. With
10 Section 702 authorities set to expire at the end of
11 2023 as well as international debate regarding U.S.
12 intelligence collection practices in recent years, now
13 is a critical moment to review current policies and
14 practices under the law and consider potential
15 additional reforms that would strengthen protections
16 for privacy and civil liberties.

17 Today's public forum is designed both to
18 inform the Board and the public as we engage in
19 oversight of the government's use of Section 702. The
20 forum will start in a moment with a keynote speech
21 from General Nakasone, Director of the National
22 Security Agency and commander of the U.S. Cyber

1 Command. It will then be followed by two panels.

2 Before we begin, I want to thank all of our
3 panelists and speakers for joining us today, as well
4 as our tremendous staff for all of their incredible
5 work in planning today's forum and making it possible
6 for us to come together today online. And in terms of
7 logistics, I want to note that today's event is being
8 recorded and the recording will be posted on the
9 PCLOB's website. So I want to turn now to General
10 Nakasone for his opening keynote remarks.

11 General Paul M. Nakasone assumed his present
12 duties as commander, U.S. Cyber Command and director,
13 National Security Agency and chief of the Central
14 Security Service on May 4 of 2018. He served as
15 commander of U.S. Army Cyber Command from October of
16 2016 to April of 2018. And previously he led the
17 Cyber National Mission Force at U.S. Cyber Command.
18 He is a native of White Bear Lake, Minnesota, and he
19 is also a graduate of Saint John's University in
20 Collegeville, Minnesota, and he holds graduate degrees
21 from the U.S. Army War College, the National Defense
22 Intelligence College and the University of Southern

1 California. So I now turn it over to General Nakasone
2 for his keynote. Thank you very much for joining us.

3 GEN. NAKASONE: Thank you, Chair. On behalf
4 of the intelligence community, I want to thank the
5 Privacy and Civil Liberties Oversight Board, as well
6 as those watching today for your interest in one of
7 the U.S. government's most important foreign
8 intelligence authorities, Section 702 of the FISA
9 Amendments Act. The authority will sunset on December
10 31, 2023, unless Congress passes legislation to
11 reauthorize it. Without Section 702, we will lose
12 critical insights into the most significant threats to
13 our nation. Our role today in talking about this
14 authority is to help inform the forthcoming
15 congressional debates.

16 You may be already familiar with the legal
17 authority. For those who are not, a brief history,
18 FISA, the Foreign Intelligence Surveillance Act dates
19 back to 1978. Title VII, which includes Section 702
20 was added as part of the FISA Amendments Act of 2008.
21 The additions to FISA were made in part to address
22 changes in communications technologies, and the

1 growing global use of U.S. communication services,
2 including some of the highest priority foreign
3 intelligence targets. This legal authority allows the
4 intelligence community to collect the communications
5 of many of our most critical foreign intelligence
6 targets located outside the United States, who use
7 these U.S. infrastructure and services to communicate.

8 FISA Section 702 is irreplaceable. It is
9 focused and limited, yet agile enough to address
10 national security threats in an ever-changing
11 technological and threat environment. It allows the
12 intelligence community to acquire the communications
13 of specific foreign actors overseas and use those
14 details to identify terrorist plots, track spies,
15 identify cyber-attacks and try to stop them, as well
16 as provide U.S. policymakers with the information they
17 need to understand a wide range of national security
18 threats.

19 As someone who was in the Pentagon during the
20 attacks of 9/11, I have a personal perspective about
21 how this authority has helped secure the nation in the
22 years since those attacks. As the commander of U.S.

1 Cyber Command, the director of National Security
2 Agency, I have seen firsthand how FISA Section 702 has
3 continued to provide critical intelligence that has
4 kept our country and our allies safe and secure.
5 Since the initial enactment of 702 in 2008, our threat
6 environment has evolved substantially.

7 Our focus has shifted from counterterrorism
8 to strategic competition. In the two decades since
9 9/11, we have seen the People's Republic of China
10 evolve as America's primary geopolitical challenge.
11 The PRC is the only competitor with both the intent to
12 reshape the international order and increasingly the
13 economic, diplomatic, military and technological power
14 to advance that objective.

15 Meanwhile, Russia continues to pose an acute
16 and ongoing threat to regional security in Europe.
17 We've also seen the nature of conflict change
18 drastically, where cyberspace is a battleground and
19 cybersecurity has become one of our most pressing
20 national security concerns. And as we have seen in
21 the last year, the world has moved into an era where
22 the shift from competition to crisis to conflict can

1 occur in weeks or days, or even minutes, rather than
2 years.

3 To address these evolving challenges and
4 continue to keep our nation secure, the intelligence
5 community needs authorities that are technology-
6 neutral and agile. FISA Section 702 is just that.
7 This authority plays an outsized role in protecting
8 the nation, providing some of the U.S. Government's
9 most valuable intelligence on our most challenging
10 targets. It provides unique information with minimal
11 risk.

12 In addition, when we look at the National
13 Security Agency's overall reporting intelligence from
14 FISA Section 702 accounts for an oversized portion of
15 reporting relative to its cost. This authority
16 provides the U.S. government irreplaceable insights,
17 whether we are reporting on cybersecurity threats,
18 counterterrorism threats, or protecting U.S. and
19 allied forces.

20 FISA Section 702 has helped us to understand
21 the strategic intention of the foreign governments we
22 are most interested in, the People's Republic of

1 China, Russia, Iran, and Democratic People's Republic
2 of Korea. We have learned about espionage plots to
3 obtain sensitive U.S. technological information. We
4 have used information from FISA Section 702 to prevent
5 weapon components from reaching hostile foreign
6 actors. We have identified threats to U.S. troops.

7 We have discovered sanction evasions and
8 disruptive foreign cyber-attacks, and intelligence
9 acquired under this authority has stopped significant
10 terrorist plots, saving American lives. I want to
11 repeat that, we have saved lives because of 702. Last
12 month, I was part of a panel at the Reagan National
13 Defense Forum with Senator Angus King about hybrid
14 warfare with other top military, government and
15 industry leaders.

16 Senator King discussed how difficult it is to
17 talk about successes in the intelligence community
18 since successes often means that terrorist plots were
19 foiled or cybersecurity vulnerabilities were patched
20 and nothing happened. As the senator noted, how do we
21 demonstrate to the public the fact that the dog didn't
22 bark in the night. It's difficult to provide you with

1 concrete examples of how this authority has helped
2 protect the country because so many of our successes
3 are just that, preventing the dog from barking in the
4 night.

5 We also have to limit what we share publicly
6 because our foreign adversaries are paying close
7 attention to how the intelligence community and most
8 specifically the National Security Agency function in
9 hopes of learning our tradecraft in evading detection.
10 But it is important for the public to understand why
11 this authority matters. So where we can declassify
12 stories that tangibly demonstrate its impact on our
13 security, we will.

14 Let me start with an example from the early
15 days of 702. In 2009, NSA discovered information in
16 702 data, indicating an al Qaeda courier in Pakistan
17 was in communications with an unknown individual in
18 the United States. We passed this information to the
19 Federal Bureau of Investigation who found that the
20 individual Najibullah Zazi and a group of co-
21 conspirators had imminent plans to detonate explosives
22 on the subway trains in Manhattan. The attack was

1 prevented. Zazi and his co-conspirators were arrested
2 and pled guilty, or were convicted of their roles in
3 the planned attack.

4 Again in 2014, FISA Section 702 provided the
5 intelligence community key insights into ISIS planning
6 and senior members of the terrorist organization,
7 including ISIS leader Haji Iman, ultimately leading to
8 the removal of Iman preventing attacks. And again, as
9 Senator King mentioned, the dog didn't have to bark.
10 The information we get from 702 today is no less
11 critical even as our focus has shifted towards
12 strategic competition. This authority continues to
13 provide critical intelligence to our policymakers.

14 Let me tell you about a few of the
15 intelligence community's most recent successes. The
16 U.S. government identified multiple foreign ransomware
17 attacks on U.S. critical infrastructure in 702 data.
18 This intelligence position the government to respond
19 to and mitigate these events, and in some instances,
20 prevents significant attacks on U.S. networks. In
21 another recent example, the intelligence community
22 used information from 702 discover -- to discover that

1 a foreign adversary had used a cyber-attack to
2 acquire sensitive information related to the U.S.
3 military.

4 And harkening back to the counterterrorism
5 origins of the authority, FISA attacks 702 information
6 contributed to a successful U.S. Government operation
7 against one of the last remaining 9/11 architects,
8 Ayman al-Zawahiri. These are just a few of the ways
9 this authority has helped keep this nation safe.
10 Stories like this are typically classified. There are
11 countless others that we cannot share without putting
12 the nation's security and classified sources and
13 methods at risk. But I hope these examples give you a
14 sense of just how vital Section 702 is to our national
15 security.

16 So I've talked about how this is a critical
17 authority and a unique authority for the U.S.
18 Government's foreign intelligence mission. But the
19 PCLOB is tasked with ensuring we are also protecting
20 the rights of U.S. persons. Civil liberties and
21 privacy are central to the implementation of FISA
22 Section 702. The law was designed with safeguards to

1 protect the rights of the American people and our
2 allies. To that end, the collection must be focused
3 on individual targets, meeting specific criteria that
4 must be documented and verified by those within and
5 outside the intelligence community. Section 702
6 cannot be used to target Americans anywhere within the
7 world, or any person outside the United States,
8 regardless of nationality, no exceptions.

9 Excuse me. Let me say that again, Section
10 702 cannot be used to target Americans anywhere in the
11 world or any person inside the United States,
12 regardless of nationality, no exceptions. The
13 government is also prohibited from targeting a foreign
14 person abroad to learn about an American. Any
15 information unintentionally collected is handled
16 consistent with specific court-approved procedures
17 intended to protect the civil liberties and privacy of
18 U.S. persons and persons inside the U.S. By executive
19 order we extend comparable protections to foreigners.

20 This authority has layers of civil liberty
21 and privacy protections embedded throughout from
22 annual training to the use of the authority that I

1 took again just last week, to policy controls on when
2 and how queries are conducted to technical controls on
3 who has access to the data and how it is secured.

4 Here at the National Security Agency, these
5 safeguards are built upon a strong culture of
6 compliance with a dedicated internal compliance group
7 focused on identifying the sources of any possible
8 incidents, and approving the protections in place. If
9 there's an incident, NSA analysts report it and it is
10 investigated by our compliance group. And after the
11 investigation is completed, our training policy and
12 technical controls are updated as needed.

13 What is most important from my perspective is
14 that these safeguards assure privacy protection at the
15 same time do not hamper our ability to produce foreign
16 intelligence. Oversight and transparency are also
17 baked into the law. All three branches of the U.S.
18 Government have a role in the oversight of Section
19 702. In the legislative branch, the congressional
20 intelligence and judiciary committees also provide
21 stringent oversight of the program, routinely
22 reviewing the government's use of the authority.

1 Within the executive branch, the Department
2 of Justice and the Office of the Director of National
3 Intelligence look at all 702 targeting, review
4 potential compliance incidents and oversee other
5 aspects of the program.

6 And of course, all of you as members of the
7 PCLOB play an important role in the ongoing oversight
8 of the program, particularly as it relates to the
9 board mission to ensure that the Federal Government's
10 efforts to prevent terrorism are balanced with the
11 needs to protect privacy and civil liberties.

12 In the judicial branch, the Foreign
13 Intelligence Surveillance Court plays a crucial role
14 in overseeing NSA's activities under FISA Section 702.
15 The FISC is comprised of Supreme Court-appointed
16 Article III judges, and provides an expressed
17 oversight in NSA's use of the authority.

18 In my personal opinion, the court applies
19 great rigor in carefully considering all information
20 bearing unlawfulness of the government's activities
21 authorized by Section 702. It conducts a
22 comprehensive review of the program every year, as

1 well as on a continual basis ensuring incidents of
2 noncompliance are addressed.

3 Over the next year, we in the intelligence
4 community will be working with our partners to ensure
5 the immense value of FISA Section 702 and the civil
6 liberties and privacy protections built into the
7 authority are clear to Congress and the public. There
8 will be conversation and debate. We welcome that.
9 Events such as this are an opportunity to engage
10 directly with people who care about these critical
11 issues.

12 So under Section 702, both national security
13 and civil liberties and privacy are preserved and
14 protected. It is an and, and not an or that connects
15 these two important goals. Neither is compromised for
16 the other.

17 702 authorities provide exquisite foreign
18 intelligence that is focused on non-US persons outside
19 the United States, and specific invaluable insights
20 that protect our nation, intelligence that cannot be
21 obtained through other means. These authorities are
22 executed by trusted intelligence community personnel

1 that are rigorously trained and certified, self-report
2 when and if they make errors and operate under
3 oversight from every branch of our government.

4 This oversight provides a verification
5 necessary to demonstrate the intelligence community's
6 lawful and appropriate use of Section 702, allowing us
7 to carry out our crucial work while ensuring our
8 rights as American citizens are protected. Thank you
9 very much for the opportunity to talk with you about
10 this important topic. I look forward for our
11 forthcoming discussions.

12 MS. FRANKLIN: Thank you so much, General
13 Nakasone. Really appreciate your remarks and your
14 taking the time to join us here today. So we are
15 going to turn next to our first panel, and I just have
16 a few housekeeping notes for those watching --
17 watching.

18 For each panel, we will first hear brief
19 opening statements from each panelist, and then my
20 fellow Board members and I will take turns asking
21 questions of the panelists with each of us asking one
22 question at a time and following that answer, moving

1 on to the next Board member. And we will cycle
2 through as many times as we have time during the time
3 for that panel.

4 So, turning to our first panel, if they can
5 all come on screen with their cameras, that would be
6 terrific. The panelist will make opening statements
7 in the following order. First, we will hear from
8 Christopher Fonzone, who is general counsel for the
9 Office of the Director of National Intelligence, or
10 ODNI. We will then turn to Julian Sanchez, who's a
11 former senior fellow at the Cato Institute.

12 We will next hear from Jeramie Scott, senior
13 counsel at the Electronic Privacy Information Center.
14 And the final panelist to make brief opening remarks
15 will be April Doss, general counsel of NSA. So,
16 again, brief opening remarks by the panelists turning
17 first to Chris Fonzone. Thank you.

18 MR. FONZONE: Thank you, Chair Franklin.
19 Can you hear me? Excellent. Well, thank you Chair
20 Franklin and all the members of the Board for inviting
21 me here today. I very much appreciate the opportunity
22 to be here with my fellow panelists to talk to you

1 about Section 702.

2 Today's discussion is an extremely important
3 one as it implicates some of our most vital interests
4 and our most cherished values. Indeed, I doubt there
5 are many people who appear on the screen today or who
6 are watching from home who would disagree with either
7 of the following two statements.

8 The United States, like all or nearly all
9 other nations, needs to collect foreign intelligence
10 in order to fulfill its obligation to keep its people
11 safe and secure. And the second statement, our
12 country's commitment to protecting individual
13 liberties limits what the Government may do in the
14 name of national security.

15 Yet, even as simple as it is to agree on
16 these basic principles, both of which we have long
17 recognized as being part of our Constitution, it can
18 often be difficult to work through how to, as I know
19 my fellow panelist April is fond of saying, weave them
20 together.

21 How should the government be allowed to
22 collect foreign intelligence? When should it be

1 prevented from doing so? When should it be required
2 to satisfy some legal burden of specific need to an
3 independent court? What happens in an emergency when
4 lives are at stake? These are not easy questions and
5 there are no obvious easy answers.

6 Luckily, however, this is an area where we
7 are very much not writing on a blank slate, for the
8 three branches of our government have long worked
9 together to develop a framework for how to advance our
10 national security needs while protecting civil
11 liberties - with a key part of this framework being
12 the Foreign Intelligence Surveillance Act.

13 President Carter recognized this when signing
14 the original FISA in 1978. "One of the most difficult
15 tasks in a free society like our own," he wrote in
16 signing statement, "is the correlation between
17 adequate intelligence to guarantee our nation's
18 security on the one hand and the preservation of basic
19 human rights on the other."

20 FISA, in President Carter's view,
21 appropriately accounted for both of these interests.
22 As he put it, FISA "sacrifices neither our security

1 nor our civil liberties and it assures that those who
2 serve this country in intelligence positions will have
3 the affirmation of Congress that their activities are
4 lawful."

5 Of course, the passage of the original FISA
6 did not end debate over these issues. Indeed, in the
7 40-plus years since FISA's passage, both technology
8 and the geopolitical landscape have continued to
9 change, and Congress has on multiple occasions
10 returned to FISA, amending the statute to recognize
11 new realities.

12 Most importantly, certainly for our purposes,
13 in 2008, Congress enacted Section 702, which
14 recognized that, due to changes in telecommunications
15 infrastructure, foreign intelligence targets - such as
16 proliferators, hackers, terrorists and spies - often
17 rely on U.S. telecommunication services.

18 With Section 702, Congress thus authorized
19 the government to seek a court order to acquire the
20 communications of these foreign intelligence targets
21 from U.S.-based telecommunications companies, while at
22 the same time requiring safeguards that protect the

1 privacy and civil liberties of U.S. persons.

2 Interestingly, President Bush's remarks on
3 signing the law that created Section 702 made a
4 strikingly similar point to the one President Carter
5 made 40 years earlier. Specifically, President Bush
6 said, "This law will protect the liberties of our
7 citizens while maintaining the vital flow of
8 intelligence."

9 To be sure, the enactment of Section 702 did
10 not end the debate over how we should collect foreign
11 intelligence while protecting privacy and civil
12 liberties. And material and important modifications
13 have been made to that Section 702 program in the 15
14 years since it became law. For example, we've
15 increased transparency around the program and put in
16 place additional protections. And, as Sharon alluded
17 to at the outset, the Board has played a vital role in
18 coming up with these additional reforms. But
19 notwithstanding these changes, the core of the program
20 Congress created 15 years ago remains the same.

21 And while the fact that we have - that we're
22 here today, of course, indicates that the debate

1 continues - there are three key points about Section
2 702 that are very much worth emphasizing.

3 First, the Section 702 program is lawful, as
4 it is clearly authorized by statute, and courts have
5 repeatedly found it to be constitutional. Indeed,
6 this is something the Board recognized when it last
7 engaged in an exhaustive review of the Section 702
8 program in 2014 and, in the years since that review,
9 the case has only grown stronger.

10 This is because since the Board's last
11 review, Congress has again reauthorized the authority
12 such that Section 702 has now been enacted and
13 reauthorized three times. Moreover, since the Board's
14 last review, Federal courts have continued to confirm
15 the board judgment as to Section 702's legality and
16 constitutionality.

17 Which leads to the second point: the Section
18 702 program is extremely valuable and effective. I
19 won't go into too much detail here, particularly since
20 the Board reached this conclusion during its 2014
21 review. But General Nakasone's opening remarks
22 provide additional details about the importance of the

1 program and how it provides critical intelligence on a
2 range of national security challenges from
3 counterterrorism to cyber to strategic competition to
4 many others.

5 And General Nakasone's remarks only build on
6 the remarks of many other IC leaders, including the
7 DNI, who have emphasized how Section 702 provides
8 critical intelligence.

9 Which brings me to a third and final point:
10 Section 702 protects privacy and civil liberties.
11 Again, General Nakasone has detailed many of the
12 extensive protections Section 702 has -- puts in
13 place. I know April Doss, who is joining me on this
14 panel, and a colleague of mine from the FBI, who will
15 be here on the next panel, will do the same. So I'll
16 not try to repeat what they will say.

17 Rather, I will simply say a few words about
18 ODNI's oversight role, which reflects the work it
19 does, integrating the intelligence community and its
20 statutory authorities and capabilities. Specifically
21 ODNI's oversight efforts largely focus on promoting
22 inter-agency coordination, prioritization, and

1 harmonization, particularly with respect to program-
2 wide modifications.

3 This means that among other things, ODNI
4 conducts in consultation with the Department of
5 Justice reviews of Section 702 taskings, coordinates
6 the provision of IC documents and briefings to
7 Congress in consultation with DOJ, and leads, in
8 consultation with DOJ, the Government's efforts to
9 provide the public with information about Section 702
10 activities, including releases of FISC opinions, joint
11 assessments, and the release of the annual statistical
12 transparency report.

13 Of course, as prior statements have made
14 clear, ODNI's work is only part of a detailed
15 compliance regime, the upshot of which is that, as
16 President Obama said in 2014, "The men and women of
17 the intelligence community . . . consistently follow
18 protocols designed to protect the privacy of ordinary
19 people. They're not abusing authorities in order to
20 listen to your private phone calls or read your e-
21 mails." These statements were true then, and they're
22 true now.

1 To be sure, the intelligence community is not
2 perfect. As President Obama also recognized in the
3 2014 remarks, "Mistakes are . . . inevitable in any
4 large and complicated human enterprise." But the
5 important point is that when the intelligence
6 community makes such mistakes, we own up to them. We
7 disclose them as appropriate to the FISC, to the
8 Congress, and to the public, and we set out to fix
9 them.

10 Which leads to my final point, which I'll
11 keep short.

12 I recognize that reasonable minds can
13 disagree about these issues. I also know based on my
14 time in government, that time in government is often
15 full of the varied joys and frustrations of trying to
16 develop practical solutions to the messy business of
17 weaving together interests, diverse interests like the
18 need to collect foreign intelligence and the need to
19 protect individual liberties.

20 Viewed through this lens, I really do think
21 702 is a thoughtful solution to a complex issue, and I
22 hope these short remarks have helped even a little bit

1 to illuminate why. Thank you and I look forward to
2 the discussion.

3 MS. FRANKLIN: Thank you. We'll turn next to
4 Julian Sanchez.

5 MR. SANCHEZ: Thanks, Sharon. And I'm
6 grateful to have been asked to join this hearing. So,
7 you know, I assume during these panels, we're going to
8 have a lot to say in the weeds about the various
9 compliance issues that have arisen over the course of
10 the 15 year history of Section 702. But I hope you'll
11 indulge with me if I lead not with a discussion of the
12 weeds, but with a somewhat more radical critique of
13 Section 702.

14 And that's that, you know, if we look at in
15 effect how it operates, we see that in or each of
16 recent years, the FISC has issued each year either one
17 or two broad authorizations for 702 acquisition. And
18 under each of those authorizations, the intelligence
19 community has exercised its discretion to designate
20 each year more than 200,000 individual foreign
21 targets.

22 And under the aegis of that authority though,

1 the targets are of non-U.S. persons located at the
2 United States, we know that a substantial number,
3 certainly in absolute terms, even if as small as a
4 percentage of the total take, substantial number of
5 U.S. person communications, certainly when their one
6 end of an international communication, but also we
7 know for many years in practice and despite in
8 explicit statutory prohibition, even many tens of
9 thousands of wholly domestic communications were
10 acquired as a result.

11 And if we sort of step back and say, well,
12 what does this look like collection on this scale,
13 where the decision about what to collect is delegated
14 to executive branch officials with only this sort of
15 programmatic authorization directly by the judiciary,
16 I think, you know, the one clear answer is that these
17 sound a heck of a lot like general warrants.

18 Now if there's a point on which Fourth
19 Amendment scholars are virtually unanimous and there
20 aren't many, perhaps, but this is one. It's the
21 original function of the Fourth Amendment, the
22 original motive behind the Fourth Amendment was

1 outrage over the general warrants and roots of
2 assistance that were prevalent during the colonial
3 era. And, you know, this is understandably sort of
4 fallen into the background of Fourth Amendment
5 jurisprudence.

6 We think today of the Fourth Amendment
7 primarily as a guarantor of an individual right to
8 privacy against unreasonable searches in effect
9 typically enforced by the exclusion of improperly
10 obtained fruits of such searches from criminal
11 prosecution.

12 But if we look, you know, closely at the
13 explicit wording of the Fourth Amendment, we get a
14 somewhat different picture, a guarantee of a right to
15 be secure, not just to individual persons, but the
16 people collectively, even though in many other places
17 in the bill of rights, the framers are happy to use
18 individual language.

19 Indeed, the original monoclausal structure of
20 the Fourth Amendment arguably does nothing but
21 prohibit general warrants. That original language
22 changed the last minute by a motion by Elbridge Gerry,

1 said that the right of the people to be secured in
2 their person's houses, papers, and effect, shall not
3 be violated by warrants issuing without probable cause
4 or particularity.

5 And the change by Gerry to a dual clause
6 structure was meant to emphasize even more strongly
7 that this was a prohibition on such general warrants
8 even issuing. And I think this is significant because
9 it gives us an understanding of what the Fourth
10 Amendment is trying to do that views the right
11 protected by the amendment as something that is
12 violated not at the time when a search is executed,
13 but when a particular kind of authorization, when a
14 particular delegation comes into existence.

15 And this is something that is reflected in a
16 lot of the founding era rhetoric around the Fourth
17 Amendment and against risk of assistance and general
18 warrants. So, James Otis, a huge influence on
19 Madison's drafting of the Fourth Amendment, argued
20 against the resistive decisions that every households
21 who are in the province will necessarily become less
22 secure than he was before this writ had any existence

1 among us.

2 James Pemberton writing on behalf of the
3 Quaker community of Philadelphia denounced general
4 warrants for conferring powers that in any free
5 society would be reprobated as overturning every
6 security men can rely on. And more than two centuries
7 later, I would note the idea that discretionary
8 surveillance can impose disparate burdens on minority
9 religious communities remains, alas, all too relevant.

10 So this is a collective or structural concern
11 that's reflected in both the original wording of the
12 Fourth Amendment, which identifies the issuing of non-
13 particularized warrants as the moment at which the
14 people's right to be secure is compromised and in the
15 more familiar current version reflecting Gary's
16 (phonetic) insistence on a more emphatic prohibition
17 on the issuance of such non-particular warrants.

18 And I think if we re-center that idea, the
19 idea that the Fourth Amendment is first and foremost
20 about barring that kind of broad delegation of
21 authority to the executive branch, we get a somewhat
22 different view of Section 702. So consider the sort

1 of a mainstay of 702 apologetics, right?

2 The people who enjoy a right to be secure
3 against unreasonable searches are the American people.
4 702 permits only the targeting of foreigners located
5 abroad, who enjoy no such protections. So there can
6 be no fundamental constitutional objection to the
7 orders that 702 authorizes.

8 I think, you know, even though of course, you
9 know, errors in implementation may themselves entail
10 Fourth Amendment violations in practice. But I think,
11 you know, by parallel reasoning we could say the
12 general warrants of such concern to the framers would
13 have been unproblematic because they didn't target
14 anyone, I think the defect in that kind of defense is
15 obvious in light of what I've said.

16 The Fourth Amendment is not a guarantee
17 against unreasonable targeting, but against
18 unreasonable searches and separately against even the
19 issuance of discretionary non-particularized warrants,
20 independent of the execution of that search.

21 Title I of FISA, FISA Classic (phonetic)
22 reflected this understanding by requiring a warrant

1 for the interception of wire communications with one
2 domestic endpoint, even if the domestic endpoint was
3 not the target of collection. To be sure the
4 discretion afforded to intelligence agencies
5 collecting communications under the aegis of 702 is
6 procedurally fettered rather than plenary.

7 But nevertheless, the statute contemplates
8 the acquisition of U.S. person communications on U.S.
9 soil on a programmatic rather than a particularized
10 basis. And I think, you know, the fundamental
11 question from a constitutional perspective has to be
12 not who is targeted, but who's communications are
13 searched and collected.

14 Now an obvious objection to this sort of
15 analysis is, well, the FISC has demonstrated its
16 willingness repeatedly to find Fourth to identify
17 Fourth Amendment violations by the intelligence
18 community in the execution of 702. It's identified
19 quite a few. So why should we think that the FISC
20 would overlook this supposed more fundamental defect
21 that I'm arguing for? And I'll suggest two reasons.

22 The first is that the Fourth Amendment has

1 been sort of a victim of its own success, right?
2 Clear rules do not tend to generate case law and the
3 prohibition on general warrants is sufficiently clear-
4 cut. Although we don't find a lot of occasions in our
5 Fourth Amendment jurisprudence for the courts to
6 emphasize it, it has faded into the background,
7 whereas the role as a kind of regulator of criminal
8 procedure has come to the forefront.

9 And second, I think the fact of the rules of
10 standing under which American courts operate requiring
11 a showing of individualized concrete harm, and the
12 fact that Fourth Amendment litigation is
13 overwhelmingly centered on questions about the
14 admissibility of evidence in criminal prosecutions,
15 creates a kind of distorting lens, right, where we
16 emphasize the individual aspect --

17 MS. FRANKLIN: Julian?

18 MR. SANCHEZ: Yeah.

19 MS. FRANKLIN: Thanks. I'm sorry. I'm going
20 to need to ask you to stop there. We need to keep the
21 openings relatively brief so that we do have time for
22 --

1 MR. SANCHEZ: Yeah.

2 MS. FRANKLIN: -- for questions. Thank you.

3 MR. SANCHEZ: So I just want to suggest that
4 that this has created a distorting lens that
5 disconnects the Fourth Amendment in -- as it exists in
6 current case law from the thing that the framers of
7 the Constitution were most centrally concerned about.
8 And I hope we can get into the weeds of specific
9 clients issues.

10 MS. FRANKLIN: Thank you. Okay. We're going
11 to turn next to Jeramie Scott for brief opening
12 remarks. Thanks.

13 MR. SCOTT: Thank you, Chair Franklin, and
14 members of the Board for holding this forum and
15 inviting me to participate. EPIC has a long history
16 of engaging with the PCLOB and on these issues,
17 particularly on Section 702 of the Foreign
18 Intelligence Surveillance Act. 702 continues to
19 implicate serious privacy and civil liberties concerns
20 and there are numerous issues to raise, one of the
21 most persistent being the warrantless backdoor
22 searches. I'll use my opening remarks to highlight

1 three other issues I hope the Board will look into.

2 One, the scope of abouts collection. Two,
3 the use of 702 collection in cybersecurity
4 investigations. And three, the need for greater
5 transparency ahead of the reauthorization debate. The
6 PCLOB should investigate the scope of abouts
7 collections, about collection sweeping communications
8 that merely reference a target and consequently it can
9 end up acquiring wholly domestic communications.

10 As a PCLOB in the Foreign Intelligence
11 Surveillance Court have both emphasized, the sheer
12 breadth of abouts collection and the extent to which
13 incidental collection is part of the parcel of abouts
14 collection results in substantial privacy violations
15 for the individuals whose personal information the
16 government incidentally collects. The NSA previously
17 failed to bring it abouts collection activities into
18 compliance with statutory and constitutional
19 requirements.

20 And for years NSA personnel recorded data
21 collected to the Section 702 upstream program using
22 U.S. person identifiers despite the express

1 prohibition against the use of these identifiers and
2 NSA's own minimization procedures. In 2017, opinion
3 deemed these queries "significant noncompliance" and a
4 "very serious Fourth Amendment issue."

5 Ultimately, the NSA determined that cannot
6 remedy the noncompliance and therefore decided to end
7 abouts collection and purge all previously collected
8 upstream data. But it's not clear that some type of
9 abouts collections is not occurring today. In a
10 October 2018 FISC opinion, there appears to have been
11 a disagreement between the Government and (inaudible)
12 in that case about whether the current limitations on
13 abouts collections apply to downstream acquisition.

14 Given this disagreement, it is crucial that
15 the PCLOB investigate and clearly define the current
16 scope of abouts collections, especially given the
17 history of persistent and significant noncompliance
18 relating to abouts collection. The PCLOB should also
19 review the use of 702 collection in cybersecurity
20 investigations. The Board's previous report did not
21 address the use of 702 in cybersecurity.

22 Since that report, the Intelligence Committee

1 has dramatically increased the use of Section 702 in
2 the cybersecurity investigations. While the
3 Government claims that Section 702 has played an
4 important role in cybersecurity investigation, there
5 is not enough public information to cooperate whether
6 Section 702 is necessary to accomplish these goals and
7 whether special safeguards are necessary in the cyber
8 context.

9 The use of Section 702 as part of
10 cybersecurity efforts raises privacy and civil
11 liberties concerns given the potential breadth of
12 collection and coring. According to the ODNI's
13 statistical transparency report in 2021, the FBI
14 conducted branch queries related to "Attempts to
15 compromise U.S. critical infrastructure by foreign
16 cyber actors." These queries include approximate 1.9
17 million in query terms relate to potential victims
18 including U.S. persons, more than all report inquiries
19 over the previous year.

20 Given this exponential increase, the PCLOB
21 should investigate and report on the use of Section
22 702 in the cybersecurity context, such reviews within

1 the scope of the PCLOB, because National Security
2 Agency has asserted that cyber-attacks are frequently
3 a vector for attacks with terroristic motives, and
4 therefore claim that cyber is an integral part of U.S.
5 counterterrorism programs. U.S. Government officials
6 have repeatedly emphasized the growing threat of
7 cyber-enabled terrorism.

8 These officials have also emphasized the need
9 to meet cyber-enabled threats with the same approach
10 as traditional counterterrorism using a whole of
11 government and all tools approach, including reliance
12 on an intelligence tool. Additionally, according to
13 the White House National Security Council, "Reliant on
14 legal authorities that make theoretical distinctions
15 between on-detect terrorism and criminal activity may
16 prove impractical." All the more reason for the PCLOB
17 to take a comprehensive review of the use of 702 and
18 cybersecurity investigation.

19 It is vital that the public understand the
20 scope of surveillance systems used in cybersecurity
21 investigations, how the data collected is used and
22 whether additional privacy and similarly protections

1 are necessary to ensure that these investigations --
2 investigative tools are not abused.

3 Last point I'll make is on the need for
4 greater transparency measures. Despite the progress
5 that has been made, the U.S. Government has not
6 provided the classified information about Section 702.
7 This lack of clarity hinders vigorous public debate on
8 the benefits and costs of these programs. Therefore
9 the PCLOB should push for greater transparency ahead
10 of the reauthorization debate.

11 In particular, the PCLOB should once again
12 seek the release of a declassified estimate of the
13 number of U.S. persons whose communications have been
14 incidentally collected pursuant to Section 702, an
15 estimate members of Congress and privacy and similar
16 groups have called for numerous times, a number the
17 Government previously said it -- previously said it
18 would provide before doing an about-face and saying
19 they could not provide it because of privacy and
20 security concerns.

21 Additionally, I urge the PCLOB to recommend
22 the further declassification of other influential FISC

1 documents and information that has bearing on the
2 public and congressional debate on the reauthorization
3 of 702. Thank you again for the opportunity to
4 participate in this panel. And I'd be happy to answer
5 any questions.

6 MS. FRANKLIN: Thank you. So the final
7 panelist to make brief opening remarks before we turn
8 to Board member questions is April Doss. I can't hear
9 you. Can others hear? You're not muted.

10 MS. DOSS: How's that?

11 MS. FRANKLIN: Great. Thank you.

12 MS. DOSS: Wouldn't -- you know, the
13 technical problems came from the NSA. Chair Franklin
14 and esteemed Board members, thank you. Thank you so
15 much for the opportunity to address and discuss FISA
16 Section 702 with you on this panel. My name is April
17 Doss, and I've been NSA's general counsel since May
18 2022.

19 Prior to becoming NSA's general counsel, I
20 worked in academia, private practice and on the Hill.
21 But I also previously worked at NSA in a variety of
22 attorney and non-attorney positions for 13 years.

1 Throughout my tenure at NSA, I've witnessed firsthand
2 the twin and deeply interwoven successes of the 702
3 program in producing critical foreign intelligence for
4 the U.S. and her allies, and in protecting the privacy
5 rights and civil liberties of persons in the U.S. and
6 around the world.

7 National security law is often thought of as
8 a balancing of the national security interests of the
9 U.S. as a whole against the rights and liberties of
10 individual people whose privacy might be impacted
11 during national security operations. However, rather
12 than accomplishing one at the expense of the other,
13 NSA has woven privacy and civil liberties protections
14 into the way in which the agency executes its core
15 national security responsibilities as signals
16 intelligence and cybersecurity.

17 NSA's signals intelligence or SIGINT mission
18 involves the use of electronic surveillance to collect
19 information about the capabilities, intentions and
20 activities of hostile foreign powers, international
21 terrorist groups, malicious cyber actors, and other
22 foreign entities or their agents to protect the U.S.

1 and its interests while ensuring that the legal
2 rights, freedoms and civil liberties of Americans
3 remain fully protected.

4 As General Nakasone said in his opening
5 remarks, Section 702 may not be used to target anyone
6 located inside the United States, nor may the statute
7 be used to target an American anywhere in the world.
8 No exceptions. Rather Section 702 of FISA provides a
9 court-supervised regime that permits the intelligence
10 community to obtain the compelled assistance of U.S.
11 telecommunications providers to target foreign persons
12 located outside the U.S. who possess or are expected
13 to communicate foreign intelligence information that
14 satisfies the carefully vetted intelligence
15 requirements of U.S. policymakers.

16 For completeness, I also note that a separate
17 legal regime embodied in Executive Order 14086
18 provides comparable protections to foreign persons,
19 because privacy interests might be impacted by NSA
20 signals intelligence activities, to include the
21 agency's 702 activities. It's not sufficient,
22 however, for me as the lawyer who works behind the

1 closed doors of NSA to simply declare that we're doing
2 enough.

3 We must show and explain to the American
4 people how the Government not only strives to achieve
5 its national security interests, but how protection of
6 constitutional rights and civil liberties is woven
7 into the very fabric of NSA's use of the authority
8 provided by 702.

9 In particular, the statute requires court-
10 approved procedures and continuing oversight by all
11 three branches of government to ensure that the
12 intelligence community's use of the authority remains
13 lawful. To its credit, this oversight regime has
14 resulted in the identification, reporting and
15 correction of compliances incidents, as well as
16 periodic adjustments to the statute and to its
17 implementing procedures.

18 For example, during the last reauthorization
19 of Section 702 in January 2018, Congress added a new
20 requirement for court-approved procedures to govern
21 intelligence agencies queries of law 702-acquired
22 information.

1 Even though 702 has been in use for over 14
2 years, it's not surprising that the law remains a
3 topic of intense interest, especially during a period
4 when it's again due to sunset unless reauthorized by
5 Congress. So with that in mind, and recognizing the
6 importance of brief remarks, I'd like to take just a
7 few moments to dispel some myths about the 702
8 program, and then briefly discuss NSA's culture of
9 compliance. Each decision to target a person under
10 Section 702 is an individualized one, made on a case
11 by case basis and subject to rigorous review.

12 Prior to initiating collection, pre-targeting
13 justifications are reviewed by at least two different
14 people beside the original analyst. Those checkers
15 evaluate the information offered and the reasons
16 provided by the analyst to confirm that the
17 information gathered demonstrates the subject at the
18 targeting as a non-U.S. person outside the U.S. and
19 who possesses or is likely to communicate foreign
20 intelligence that is responsive to those intelligence
21 needs.

22 After collection is begun, as analysts must

1 document their post-targeting analysis on a routine
2 basis. If an error is discovered, analysts must self-
3 report that error, so it can be tabulated and
4 ultimately forwarded to external overseers. But self-
5 reporting is not the only checking mechanism.
6 Compliance officers, auditors, lawyers and
7 investigators continually review and re-review
8 targeting decisions and make sure that analysts acts
9 appropriately or in the case of a compliance incident
10 that the incident is promptly reported and addressed.

11 In recent years, these compliance incident
12 reports have been made more accessible to the public,
13 as demonstrated by the thousands of pages of court
14 decisions and other materials that the intelligence
15 community has declassified and released over the past
16 several years. This overall increase in transparency
17 demonstrates the extent to which the compliance regime
18 is functioning effectively and robustly.

19 The Foreign Intelligence Surveillance Court
20 takes its role in the FISA process extremely
21 seriously, requiring all incidents of 702
22 noncompliance to be reported immediately to the court,

1 whether they involve U.S. or non-U.S. persons, and it
2 regularly mandates the government to correct incidents
3 of noncompliance to the court's satisfaction.

4 Perhaps the most difficult part to convey
5 through facts or figures or statistics is NSA's
6 culture of compliance. This culture of compliance
7 stems from a deep respect for the U.S. Constitution
8 and adherence to the rule of law, which is woven into
9 everything that we do. Even after many years at NSA,
10 there's one anecdote that stands out for me as
11 representative of that culture of compliance.

12 It was 2005 and I had just started a new
13 position in NSA's Office of General Counsel, where I
14 would be advising analysts on intelligence law. As I
15 was awaiting my first assignments, my supervisor
16 handed me a stack of thick paper bound volumes. These
17 were the complete five volume report at the Church
18 Committee, the precursor to the Senate Select
19 Committee on Intelligence, documenting its findings
20 from the mid-1970s investigation into spying on
21 Americans by the U.S. intelligence community, and the
22 1950s, '60s and '70s.

1 My new boss told me to read the reports and
2 understand that history with a particular eye to the
3 parts that focused on NSA. Although it had been 30
4 years since that report was published and almost 30
5 years since FISA had been enacted, reading those
6 reports was part of my on-the-job training for the
7 work that I would be doing. Stories like this are
8 common at NSA across all organizations.

9 NSA's memory of past events has created a
10 profound respect for mechanisms of accountability,
11 supervisors, senior analysts, lawyers, compliance
12 officers, technical specialists, and others make sure
13 that all of NSA's formal compliance programs are
14 supplemented with a living history and institutional
15 memory in which a commitment to protecting privacy and
16 civil liberties forms the bedrock of everything we do.

17 MS. FRANKLIN: Thank you.

18 MS. DOSS: (Inaudible).

19 MS. FRANKLIN: If I could -- if I can ask you
20 to please wrap up. We -- board members are -- there
21 are five of us more -- to ask more questions. Thank
22 you.

1 MS. DOSS: Thank you. Thank you again, for
2 inviting me to speak at this forum. And I look
3 forward to a thought-provoking discussion.

4 MS. FRANKLIN: Thank you. Thank you to all
5 our panelists. And sorry, with five of us and time
6 being short, we're going to cycle through the board.
7 We're going to switch our order for the two panels.
8 So hopefully, we all have a chance to ask multiple
9 questions. And we'll go one question at a time. For
10 this round, we're first going to get a question from
11 Travis LeBlanc.

12 MR. LeBLANC: Thank you very much, Chair
13 Franklin. And thank you to all the panelists for
14 joining us today. I appreciated your remarks as well
15 as those of General Nakasone. Very much appreciate
16 everyone being here today. There is no doubt Section
17 702 collects a vast amount of information as publicly
18 relayed in the Board section 2014 -- in the Board's
19 2014 report on Section 702. In that same report, the
20 Board noted that some of the information in -- under
21 Section 702 includes U.S. person communications, or
22 information of or concerning U.S. person information.

1 Today, Section 702 authorize executive branch
2 officials to make targeting decisions on specific
3 selectors without any judicial oversight. There is no
4 individual or particularized basis for the targeting
5 decisions overseen by an independent magistrate or
6 judge. Mr. Sanchez, do you believe Congress should
7 require the intelligence community to obtain a FISA
8 order or warrant to run queries on U.S. persons under
9 Section 702?

10 And if so, do you believe that the
11 Constitution requires an order or warrant for such
12 queries? I recognize the significance and import of
13 this issue. And while directing the question to Mr.
14 Sanchez, invite any panelists to respond as well.

15 MR. SANCHEZ: You know, I do and in light of
16 certainly of the -- the enormous scale of collection.
17 And in particular, given the sort of dual-hatted role
18 of the FBI, which has access to these -- this intake
19 database. So we have this sort of enormous scale of
20 collection nominally for foreign intelligence
21 purposes. And we see a pattern of very large-scale
22 querying by FBI on the order of, in some cases,

1 millions of queries per year, sometimes in very large
2 batches of whose ability to satisfy even the internal
3 querying standard is dubious.

4 I think it suggests the need to involve a
5 magistrate for those purposes. Two reasons, in
6 particular I'd say one, after the 2018 imposition of
7 requirements for FBI analysts to return to the FISC
8 when they need to run queries for purely criminal
9 investigative purposes, we find reports after the fact
10 that query seemed to have continued for those purposes
11 without obtaining the required authorization from the
12 FISA court. And also because, you know, the FISC
13 itself repeatedly, after being often belatedly
14 notified about compliance issues have said that
15 they've found what appeared to be on the FBI side,
16 either widespread misunderstanding of or indifference
17 to the fundamental querying roles and key terms such
18 as likely to return by information related to foreign
19 intelligence, that had been essential to the querying
20 policies since the inception of the -- of those
21 programs, you know, more than 14 years ago.

22 So I think, you know, what it demonstrates

1 pretty well, is it delegating this kind of decision-
2 making authority to agents of the executive branch
3 with oversight only after the fact and kind of on the
4 honor system has not worked out very well. I think
5 we've sort of tried compliance whac-a-mole for long
6 enough. And, you know, the evidence is that the
7 issues keep arising.

8 MS. FRANKLIN: Thank you. So the next
9 question is from Beth Williams.

10 MS. WILLIAMS: Great. Good afternoon, and
11 thank you to all of our panelists for being here
12 today. My questions for Mr. Fonzone. Some
13 commentators have recommended that the administration
14 should be open to accommodating the concerns of
15 numerous members of Congress about the improper use of
16 intelligence authorities for partisan reasons,
17 specifically with regard to crossfire hurricane.

18 It's my understanding that the improper use
19 of authorities related to that investigation did not
20 implicate Section 702 authorities. Can you comment on
21 whether that is accurate? And can you also comment on
22 what protections exist or should exist to ensure that

1 Section 702 is not weaponized (phonetic), either
2 wittingly or unwittingly, in service to any partisan
3 purpose?

4 MR. FONZONE: Sure. Thank you. Thank you,
5 Board Member Williams for that question. Yes. First,
6 I can confirm that the high profile discussion of a
7 FISA compliance incident with respect to crossfire
8 hurricane did not involve the Section 702 program.

9 I also can confirm that the IC is - and I
10 would ask April to weigh in here, as she talked about
11 it - and I'd say it's culture of compliance.

12 I think that's a culture of compliance that
13 exists across the intelligence community, and the
14 intelligence community is very much focused on being
15 scrupulously apolitical in how it wields its
16 authorities. I think we recognize the power of those
17 authorities and that they have to be wielded in a way
18 that can maintain the trust of the U.S. people. So I
19 think leads to your last point, which is, although I
20 think that the IC already operates in a scrupulously
21 apolitical way, the DNI has made clear that we're open
22 to discussing reforms with Congress that would improve

1 -- that would preserve the program's efficacy while
2 adding to civil liberties and privacy protections.

3 And if there are reforms of that nature, that
4 would address the concerns that members of Congress
5 have to make clear the fact that's already true, which
6 is that the IC operates apolitically, I think we'd be
7 open to having that discussion.

8 MS. FRANKLIN: Okay. So the next question is
9 my turn. So I'm going to turn to April Doss, please.
10 So as you're well aware, before the spring of 2017, as
11 part of upstream collection, the NSA conducted what
12 has been called about collection where NSA collected
13 not only communications to or from a target, but also
14 communication about targets, such as where a target's
15 e-mail address appeared in the body of an e-mail.

16 And in 2017, NSA announced that it had
17 suspended that collection, essentially noting that the
18 number of compliance incidents and the challenges in
19 complying with the rules, the value of the about
20 collection was not sufficient to overcome those. Then
21 when Congress reauthorized Section 702 in January of
22 2018, it required that if NSA wants to restart about

1 collection, the government must first get approval
2 from the FISA Court and then must also notify
3 Congress.

4 To date, as we understand it, NSA has not
5 restarted about collection. What can you tell us
6 regarding whether NSA has any plans to resume about
7 collection or what the standards or reasons would be
8 for NSA to seek to restart about collection or whether
9 NSA would oppose a permanent end to about collection?

10 MS. DOSS: With respect to the last part of
11 your question, of course, NSA is delighted to take
12 part in any classified and unclassified conversations
13 with the Board. And certainly with the larger set of
14 stakeholders, as we look at what reauthorization could
15 potentially look like. As Chris mentioned, certainly,
16 the intelligence community is looking to work actively
17 with the Hill. We will be looking to the
18 administration's position on this as on all other
19 matters. And NSA's role was simply to be informed
20 that discussion.

21 I would note that, you know, in General
22 Nakasone's remarks, you know, he pointed to how

1 quickly the intelligence environment can change. He
2 referred -- he gave the example of how quickly we can
3 move from competition to crisis to conflict. And I
4 think that it'll be important as we have those
5 conversations about what additional reforms to the
6 statute might look like that those conversations take
7 into account the agility that the intelligence
8 community will be able to need to retain in order to
9 carry out new programs or new techniques, if needed.
10 And as properly authorized as you pointed out, of
11 course, most importantly, NSA is not currently
12 engaging in any abouts collection. And if it had an
13 intention to do so would go to the FISC, would notify
14 Congress.

15 So that is the status that we're in. And of
16 course, we would welcome the conversation in
17 classified settings, with the Board, with ODNI and
18 with the Department of Justice and others, on what the
19 implications of that kind of statutory change could
20 potentially be.

21 MS. FRANKLIN: Thank you. The next question
22 is from Ed Felten.

1 MR. FELTEN: Thank you. And let me join my
2 colleagues in thanking all of the panelists and
3 General Nakasone for your remarks and your appearance
4 and willingness to answer our questions today. I have
5 a question for April Doss, which relates to the
6 question of how NSA might be able to estimate the
7 prevalence of U.S. person information in Section 702
8 collection.

9 This was a recommendation of the 2014 PCLOB
10 report on Section 702, as you know. And as you also
11 know, there's been a bunch of back and forth with
12 Congress and others about this question. And my
13 question for you is not -- today is not to debate the
14 ins and outs of this. But simply to ask, what might
15 NSA do? What might Congress do? What might we at the
16 PCLOB do to move this issue forward? In light of the
17 obvious value to Congress and the public from having
18 insight into the extent of incidental collection of
19 U.S. person information and the practicalities of the
20 issue. What might be done to move this issue forward?
21 And I think you're muted.

22 MS. DOSS: Thank you for that question. We

1 welcome discussion on any viable solution that's
2 accurate, repeatable and focuses on foreign
3 intelligence. Of course I know that in the next panel
4 there'll be one of the presenters, one of the co-
5 authors of the paper about One Proposed Approach
6 (phonetic).

7 You know, in the past several years, NSA has
8 provided the congressional oversight committees and
9 the PCLOB with detailed explanations of methods that
10 we have tried to use to estimate incidental
11 collection, what metrics were produced and why those
12 failed to produce an accurate or reliable metric.

13 As we've undertaken efforts over the years to
14 try to do that, our efforts have been guided by three
15 principles. First, that the approach should produce a
16 metric that's meaningful and reliable. The approach
17 would need to be replicable and mathematically sound.
18 It would need to make clear what's being counted and
19 what's not being counted. And it would need to
20 produce a number that makes a genuinely useful
21 contribution to the public discussion on 702
22 reauthorization.

1 Second, of course, the approach would need to
2 safeguard civil liberties and privacy. As you know
3 that's been one of our chief concerns is how to do
4 that counting without creating a focus on U.S. person
5 information, which, of course, is not our role. We
6 are a foreign intelligence agency that stands at the
7 shores of the nation and looks out.

8 And then third, of course, the approach has
9 to be feasible, and shouldn't unduly divert resources
10 from mission-essential functions. Those three
11 principles have guided all of the approaches we've
12 taken. And again, we welcome any discussion about
13 viable -- potentially viable solutions that would be
14 accurate and repeatable and focus on the foreign
15 intelligence.

16 MS. FRANKLIN: Thank you. And next, we'll
17 turn to Rich DiZinno.

18 MR. DiZINNO: Thank you, Chair Franklin. And
19 again, I join my colleagues in welcoming all the
20 panelists, and thank you for your time again. My
21 question is for April Doss. April, thank you, again,
22 for being here.

1 We've heard some discussion about the
2 evolving cybersecurity threat and addressing that
3 threat using Section 702 authorities. As we all know,
4 the origin of intelligence collection activities that
5 have since been codified under Section 702 arose in
6 the aftermath of the 9/11 attacks. And the original
7 sort of use case for operationalizing type of
8 collection that's been since codified was to address
9 that post 9/11 threat.

10 Without obviously getting into classified
11 details, can you talk about the cybersecurity threats
12 that we face as a country? How the use of Section 702
13 surveillance is being used to help meet those threats?
14 And can you also touch on the differences in
15 implications on privacy and civil liberties? Namely,
16 as 702 surveillance authority is applied to address
17 cybersecurity threats as opposed to sort of
18 "Traditional terrorist threats," what are the relative
19 impacts on privacy and civil liberties concerns in
20 those two different contexts?

21 MS. DOSS: Thank you for that question. I
22 think, you know, as we look at the mission impact,

1 General Nakasone, just a few minutes ago, gave some
2 examples of some of those key intelligence threats to
3 the U.S. national security, threats to critical
4 infrastructure, and the ways in which 702 has helped
5 to counter those, for example, through identifying
6 foreign ransomware attacks on critical infrastructure,
7 and cyber-attacks designed to acquire sensitive
8 information related to the U.S. military.

9 If we look at the structure of the law
10 itself, when Congress passed 702 in 2008, that
11 decision was really driven by changes in global
12 telecommunications infrastructure. Those changes
13 remain equally relevant today. And one of the things
14 that I think we can see echoed in the director's
15 remarks a few minutes ago is that this authority has
16 proven to be remarkably adaptable, and remarkably
17 versatile. The authority is underpinned by the ways
18 in which the telecommunications infrastructure had
19 made the old Title I FISA framework, not obsolete, but
20 less applicable to certain types of intelligence
21 activities.

22 So Title I and the probable cause to believe

1 that an entity is an agent of a foreign power and
2 those Title I warrants remain a core backbone of FISA.
3 But the changes in telecommunications infrastructure
4 that were taking place by the early 2000s drove this
5 change to recognize that the intelligence community
6 needed an additional set of tools. And what we found,
7 what the director alluded to, is that these tools have
8 been highly effective against a variety of targets.

9 In addition to counterterrorism, has been
10 highly effective in looking at matters relating to
11 cybersecurity and relating to broader national
12 interests, and the kinds of intelligence priorities
13 that we have in strategic competition with some of
14 those key foreign adversaries.

15 So we would really welcome an opportunity to
16 talk with you in more detail in a classified setting
17 about how this looks in the cybersecurity context, and
18 then how that might be -- how that might be conveyed
19 appropriately in unclassified ways to provide
20 additional context or clarity or transparency for the
21 public at large.

22 MS. FRANKLIN: Thank you. I don't know how

1 many full cycles we will get. But we're going to keep
2 going until the time is up for this panel. So back to
3 Travis LeBlanc.

4 MR. LeBLANC: Thank you. I have a question
5 for Mr. Fonzone. On Subsection F2 of I think Section
6 1881 FISA, requires the Federal Bureau of
7 Investigation in criminal, non-national security
8 investigations to obtain an order from the FISC prior
9 to making U.S. person queries. I believe this is the
10 provision that Mr. Sanchez was referring to earlier in
11 his remarks, in which he I believe suggested that this
12 authority has not been used by the FBI. Is that true?
13 And if so, why not?

14 MR. FONZONE: So I think the -- we will have
15 a colleague of mine from the FBI on the next panel. I
16 think a question like this directed to the FBI's
17 activities under the statute is probably best directed
18 to him, Board Member LeBlanc. I'm happy to talk a
19 little bit about why the FBI may conduct a U.S. person
20 queries and some of the things ODNI has said about
21 that in the past. But I think the specific question
22 with respect to the FBI's behavior under that

1 statutory provision is probably best directed to my
2 colleague from the FBI in the next panel.

3 MS. FRANKLIN: I'm going to let Travis go
4 again, if you want to quickly since you didn't get it.

5 MR. LeBLANC: Sure. I will go again.

6 MS. FRANKLIN: Oh, you have to be quick.

7 MR. LeBLANC: I'm very quick all the time.
8 Jeramie, Mr. Scott, you have several times in I
9 believe your remarks mentioned that you believed it
10 was important that there be safeguards that you would
11 like to see implemented in the context of cyber. And
12 I'm wondering if you have any thoughts on the kinds of
13 safeguards that you believe should be implemented
14 around the use of Section 702 in the cyber context?

15 MR. SCOTT: Thank you, Board Member LeBlanc,
16 for the question. Let me first, you know, as I
17 alluded to, we need actually more information about
18 how cyber is being used in the first place to
19 adequately narrow down what type of protections may
20 need to be in place. Some of the issues there is kind
21 of the scope of collection that's happening under
22 cyber. And then how that information is being used

1 after the fact. Just like you have incidental
2 collection generally with 702, that information is
3 used.

4 Post-collection, there needs to be, I think,
5 a review of how that information from the cyber
6 context is being used and probably needs to be a
7 narrowing of how that information is being used. And
8 so it's only used for the kind of specific cyber
9 context. And it's not then being used beyond that
10 context, because just like the 702 in general, with
11 the cyber, there's -- often it's an incidental
12 collection of information from U.S. persons, including
13 communications.

14 And there's -- and it's sort of a black box
15 right now, I think, to the public, in terms of the
16 scope of cyber, the privacy and civil liberties
17 implications of cyber. So I think some of the same
18 kind of protections that we see generally need to make
19 sure they're applied to the cyber context, whether
20 it's memorization (phonetic), whether it's the
21 narrowing of the use of that data. Or sometimes
22 perhaps even though requirement, a new requirement for

1 a warrant to search that information as discussed
2 earlier in 702 in general.

3 MS. FRANKLIN: Thank you. Beth -- back to
4 Beth Williams.

5 MS. WILLIAMS: So this question is for April
6 Doss. April, for Americans who were very concerned
7 about privacy threats, and there are many Americans
8 who are, can you describe what you see is the threat
9 to U.S. person's privacy from hostile foreign actors?
10 And can you share if and how does Section 702 assist
11 the United States in protecting the privacy of U.S.
12 persons from foreign actors?

13 MS. DOSS: Thank you for that question. It
14 is such an important one, you know, at the beginning
15 of the day, at the end of the day, 702 is all about
16 protecting the U.S. and her allies. And that includes
17 protecting the U.S. people from all threats.

18 And when we use 702 to protect -- to identify
19 and protect specifically against foreign threats,
20 absolutely, we are looking at what some of these
21 adversary nations are doing to try to gather
22 information about American targets for

1 counterintelligence purposes. We are using it for
2 force protection purposes. 702 is critical to support
3 to military operations. It is critical to
4 understanding the ways in which foreign adversaries
5 are carrying out a whole host of activities that raise
6 privacy and civil liberties threats to the American
7 people.

8 And here, again, we would be happy to share
9 additional information in a classified setting around
10 what those threats look like and work with you to
11 determine how best to increase transparency on the
12 ways in which 702 is a key protection for the public
13 against foreign threats to the nation, including the
14 security of individual Americans.

15 MS. FRANKLIN: Thank you. Okay. So the next
16 question is from me. And I'm going to turn to Julian
17 Sanchez. So you spoke in your opening remarks about
18 your concerns about overbroad collection under Section
19 702, without having any, you know, particularized
20 findings about targets. Some of the changes that some
21 civil society advocates have urged are to narrow that
22 scope of collection by either requiring that targets

1 be an agent of a foreign power or narrowing the
2 definition of foreign intelligence that can be subject
3 to 702 collection.

4 We have had some change with regard to the
5 new executive order that President Biden issued in
6 October on enhancing safeguards for United States
7 signals intelligence activities, which specified that
8 all signals intelligence can only be conducted
9 pursuant to a specified list of 12 legitimate
10 objectives.

11 I'm wondering in this context if you have any
12 particular recommendations you would urge with regard
13 to targeting under Section 702, to address some of the
14 concerns that you made? What specific reforms would
15 you want PCLOB to recommend in this regard?

16 MR. SANCHEZ: Sure. So to say a couple of
17 things. So, first, yeah, I think insofar as the FISC
18 itself has discussed the foreign intelligence sort of
19 carve-out from the warrant requirement in terms of
20 collection directed at suspected agents of a foreign
21 power, I think that's a disconnect between the sort of
22 parameters of the space in which the executive branch

1 has a broader authority to act with more limited
2 supervision and the statutory text.

3 So to the extent that FISC itself has said,
4 you know, the conditions are less stringent in cases
5 involving not surveillance of any international
6 communication, but specifically surveillance targeting
7 agents of foreign power, those parameters should be
8 reflected in the statutory contours. And maybe that
9 in terms of specific authorizations issued by the
10 FISC, that is reflected. But I think, you know, if
11 it's important enough to be part of the parameters of
12 the less stringent requirements for judicial
13 oversight, that ought to be reflected in the statute.

14 Another thing I'd say is, you know, to the
15 extent that the public pitch for 702 was really
16 initially about, you know, as we all kind of think
17 back and recall, you know, 2005, 2007, 2008, it was
18 really centrally about an issue that had arisen with
19 trends in communications, right? The argument that
20 was made to the public and to Congress was there is a
21 problem with asynchronous Internet communications such
22 that what is fundamentally a foreign to foreign

1 communication transiting United States looks when you
2 carve it into asynchronous pieces, like two one-end
3 domestic wire communications, right?

4 The e-mail goes to Google. And then the e-
5 mail goes from Google's somewhere else as part of a
6 separate wire communications. There were instances
7 where FISC judges were treating that essentially as
8 two one-end domestic communications. And we needed a
9 fix for that.

10 And I agree we needed to fix for that. But
11 the solution we ended up with was significantly
12 broader, where we didn't just say, look, you know, we
13 need to understand what is fundamentally a transiting
14 communication or areas where, you know, we may not
15 know in advance the location of one endpoint of the
16 communication. And what we got instead was a fix that
17 also moved one end domestic communications within the
18 potential ambit of 702 that had traditionally required
19 a more individualized FISA warrant when they were
20 known to be one end domestic wire communication. It's
21 like one thing we can do there is bring, you know,
22 what was intended as a fix to that particular kind of

1 problem much closer to that and segregate the issue
2 of, you know, genuinely international communications
3 transiting through the U.S. from collection of
4 communications where we have a known U.S. participant
5 or endpoint, ideally, you know, at the collection
6 stage and then certainly in particular at the querying
7 stage when that's not feasible.

8 MS. FRANKLIN: Thank you. Turning back to Ed
9 Felton.

10 MR. FELTON: Thank you. My next question is
11 for Jeramie Scott and it relates to Abouts Collection.
12 In your opening statement you mentioned a FISC
13 proceeding raising questions about the boundaries of
14 what constitutes Abouts Collection and thank you for
15 raising that issue for us. But I'd like to ask a
16 question Abouts Collection more generally and in
17 particular given that NSA stopped the Abouts
18 Collection almost 6 years ago now. But NSA has also
19 stated repeatedly that there is value in retaining the
20 option to restart Abouts Collection should conditions
21 change. And given as well that there is a requirement
22 in the current statute to notify -- that NSA notified

1 Congress before resuming.

2 I just like to ask what you -- for your
3 opinion on that regime of allowing a restart with
4 notification to Congress. How would you suggest
5 Congress might approach the question of what to do
6 about Abouts Collection in -- as it considers the
7 statute?

8 MR. SCOTT: Board Member Felton, thank you
9 for the question. I mean, first, I would like to see
10 a permanent ban on Abouts Collection by understanding
11 that, you know, there may be value that I'm not
12 exactly privy to. I would also like to see that if
13 Abouts Collection began again, an automatic trigger
14 for review by the board itself, not just to inform
15 Congress, but an actual look at how this is being
16 implemented and, you know, reviewing of some of the
17 issues we've seen before with Abouts Collection. It's
18 obviously, you know, constitutionally bumps up against
19 or that Abouts Collection bumps up against
20 constitutionality because of its, you know, collection
21 of information incidentally of U.S. persons.

22 So, I would like to see if that ever happens,

1 Abouts Collection begin, an automatic review by the
2 PLCOB or another independent oversight entity for that
3 reason, because it poses so many issues with respect
4 to privacy and civil liberties. And to my point that
5 I made earlier in my opening remarks, right now, it
6 would be helpful for the board to review the kind of
7 disagreement that was in that opinion where the
8 (inaudible) actually thought that what was happening,
9 what the NSA was doing, actually triggered the kind of
10 requirements of Congress related to Abouts Collection.
11 And obviously the government disagreed and the FISC
12 ruled in the government's favor. There's obviously a
13 disagreement there that would be helpful for an
14 independent oversight board to look at and make an
15 informed determination on and present some of that
16 information to the public, hopefully.

17 MR. FELTON: Thank you.

18 MS. FRANKLIN: Thanks. Okay. So, we're just
19 going to have time to finish out a second round of
20 questions. So, Rich DiZinno, hopefully have a quick
21 question and answer and then we'll conclude this
22 panel.

1 MR. DiZINNO: Sure. Thank you, Sharon. I
2 guess, I'll turn back to Abouts and ask you, April,
3 again, in terms of at the time that NSA ended the
4 practice of Abouts, NSA made that decision in the
5 midst of some public discussion, although limited in
6 an unclassified fashion some of the complications
7 involved in that decision. My understanding is that
8 those balancing factors included operational
9 difficulty, compliance issues that arose as a result
10 of that operational difficulty and weighing the
11 overall benefit of the intelligence value gain from
12 using that method of collection. Can you talk about
13 that and talk about sort of those countervailing
14 factors that NSA evaluated in making that decision?

15 MS. DOSS: So, I think you've identified
16 exactly those factors that were taken into
17 consideration. You know, when I mentioned earlier
18 NSA's culture of compliance, we really weave together
19 this commitment to Foreign Intelligence Collection and
20 the commitment to Protection of Privacy and Civil
21 Liberties. And we try to continuously improve our
22 compliance mechanisms and programs. And we try to

1 take lessons learned from programs where we've had to
2 carefully assess what is the intelligence value and
3 how does that weigh against the risk to privacy and
4 civil liberties. And so the Abouts Collection, as you
5 pointed out, was an instance where in weighing all of
6 those factors. The course of action that was most
7 consistent with all of those values and aims for the
8 government was indeed to cease the Abouts Collection.

9 So, as we try to -- and we try to take that
10 approach to all of our activities to say from a
11 compliance perspective, what do we have in place in
12 terms of training of people, in terms of policies and
13 processes, in terms of technical compliance measures?
14 When we're looking at any mechanism, any particular
15 approach to implementing 702, we look at how do we
16 weave together the intelligence activity with the
17 compliance activity and where we find that as in the
18 instance of Abouts that the weighing of those factors
19 was proving challenging. We self report that, we work
20 with the Board, with our congressional overseers, we
21 work with DOJ, we work with ODNI, to determine what is
22 the best course forward. So I hope that helps answer

1 the question.

2 Again, as has been pointed out, Abouts
3 Collection certainly is paused. We would of course
4 notify the FISC and Congress if there was an intention
5 to resume it and of course we're quite happy to
6 continue having much more detailed conversations with
7 you all at a classified level.

8 MS. FRANKLIN: Okay. Thank you very much to
9 all of our panelists. Very much appreciate all of
10 your remarks and your answers to our questions. And
11 I'm going to say thank you for joining us.

12 And we're going to welcome in our second
13 panel. So, if our panelists for the second panel can
14 come on camera. We are, as with the first panel,
15 going to begin with brief opening remarks by each of
16 the panelists. And I'm going to urge you to please be
17 brief, so we can make sure to have time for questions
18 from all of the board members. There are five of us
19 who are all eager to ask you all questions. And we're
20 going to, again, cycle through each board member,
21 asking one question at a time. We're going to reverse
22 the order and I will note who is going to be asking

1 the next question each time.

2 So, we're going to hear from our panelists
3 for the opening remarks in alphabetical order.

4 First we will hear from Cindy Cohn, who's
5 Executive Director of the Electronic Frontier
6 Foundation or EFF. We will next hear from Mike
7 Herrington, Senior Operations Advisor at FBI, then
8 we'll hear from Professor Jeff Kosseff, of the U.S.
9 Naval Academy. And the last speaker for opening
10 remarks will be Professor Jonathan Mayer of Princeton
11 University. So, turning first to Cindy Cohn. Thank
12 you.

13 MS. COHN: Hi. Thank you very much, the
14 Board, for the opportunity to share EFF's views on
15 Section 702. We want to especially thank the Board
16 for its past work on 702, nearly a decade ago now. It
17 was critical to us as an organization that was
18 struggling hard to get the American people and the
19 judiciary to even understand that the Section -- what
20 became the Section 702 program existed happened. And
21 it was a critical moment in order to bring this
22 program, which, you know, we should all be reminded,

1 occurred without legal authorization for many years
2 under some semblance of the Rule of Law.

3 To the end, we hope that the Board can
4 reanimate its role in shedding much needed light on
5 this large and very expensive program, including not
6 just how 702 is being used in practice, what kind of
7 mission creep has occurred from the original
8 antiterrorism justification. I heard strategic
9 competition just now as yet another thing that gets
10 layered on top of what originally was supposed to be
11 narrowly laser focused on stopping terrorism. And how
12 U.S. persons and non-U.S. persons are impacted by it?
13 And especially, I hope, articulating the severe, if
14 not fatal, barriers to real accountability and
15 oversight programs that occur under 702 today,
16 especially in the context of individual is seeking to
17 redress for the way the program has impacted them.

18 We believe that such an independent
19 articulation is crucial to congressional consideration
20 of whether to renew 702. And if it is to be renewed,
21 any changes to it. Without that there's a very real
22 risk that renewal will be based, once again, on

1 largely one-sided limited disclosures of information
2 from the obviously self-interested IC. I don't mean
3 that in a way to say that they are wrong, it is their
4 job to try to make sure that these authorities
5 continue, and that they can continue on what they're
6 doing, that's their job. I understand being
7 somebody's lawyer. But that means that there needs to
8 be a third-party that is impartial that can evaluate
9 those claims and not just one sidedness here.

10 Past experience shows that these kind of
11 disclosures have not been sufficient to give the
12 American public or Congress a clear-eyed view of
13 what's going on. And they shouldn't be -- continue to
14 do this as we head towards renewal, much less
15 protecting the public interest.

16 Additionally, while there are a lot -- there
17 are many problems with 702 itself, and I will talk
18 about some of those, I really want to urge the Board
19 to consider how governmental secrecy now renders moot
20 many of the accountability and oversight mechanisms
21 for national security surveillance that exist on paper
22 in FISA, as well as in the U.S. Constitution. As the

1 -- this board is well aware, EFF's highest priorities
2 for the last 2 decades has been ensuring that
3 individuals can seek judicial accountability for
4 violations of their constitutional and statutory
5 rights committed through the government's warrantless
6 foreign intelligence surveillance inside the United
7 States. And we have led to key litigation
8 specifically about 702 surveillance happening versus
9 AT&T, which is about the surveillance that existed
10 before it came under 702 authority, and then 1702 was
11 enacted, Jewel versus NSA, because Congress in its
12 wisdom granted something called Retroactive Immunity
13 to the telephone companies to try to protect them from
14 the rampant legal violations that had occurred prior
15 to Section 702's passage.

16 I think we have to be honest at this point,
17 that the U.S. has de facto created a national security
18 exception to the U.S. Constitution. And this isn't
19 solely or to me even primarily about legalities. The
20 American people and indeed people all around the world
21 have lost the ability to have a private conversation
22 over digital networks.

1 702 is a mass monitoring infrastructure that
2 subjects people's communications to NSA review,
3 whenever the internet happens to route their
4 communications through key infrastructure points,
5 mainly on or near the U.S. borders. This impacts,
6 admittedly, millions of Americans and also untold
7 numbers of non-Americans, the numbers of which as you
8 know, we cannot even tell you because they can't even
9 figure it out. But these people are impacted solely
10 because they use the internet in ways that pass
11 through these monitoring stations. This surveillance
12 is suspiciousless and it's warrantless. And any
13 analysis of the NSA's surveillance that starts after
14 collection is missing this critical piece, which I
15 think is important for civil liberties as (inaudible)
16 were just basically understanding what's really going
17 on.

18 So, regardless of what happens after this and
19 digital monitoring and collection, this is a
20 fundamental change in the rights of all people around
21 the world, including Americans to have a private
22 conversation and should be recognized as neither

1 necessary nor proportionate under international Human
2 Rights Law. You know, this stretches far beyond the
3 narrow special needs doctrine exception to the Fourth
4 Amendment that we've seen so far in Fourth Amendment
5 Law. I'm happy to go in that more detail, but that
6 will take way longer than 5 minutes.

7 Additionally, it's now clear that Americans
8 have no avenue to remedy this problem, and that the IC
9 has obfuscated and blocked transparency into its
10 activities such that due process, separation of powers
11 and other core American values are at risk. They're
12 simply not available in the context of the NSA spying.
13 And of course, it's clear that the fruits of this
14 surveillance don't just stay with the NSA, as
15 wonderful as I'm sure those individual people are.
16 The fruits also stretch over to the FBI, which means
17 they are available for prosecution and indeed have
18 been used for prosecution in situations in which, as
19 far as I'm aware, no defendant has ever been given
20 access to the information that went into their
21 prosecution.

22 So, I want to talk about a few things that I

1 think this that this Board ought to honestly be honest
2 about and recognize. First, this is mass
3 surveillance, not targeted surveillance. The sheer
4 numbers and admitted mechanisms of upstream removes
5 the basic ability for people to have a private
6 conversation. This is mass surveillance, regardless
7 of how targeted things are once it gets initially
8 collected or reviewed.

9 Second, let me see if I can move more
10 quickly. Treating the monitoring of traffic as a
11 transit keys infrastructures, if it is the same thing
12 as listening in on Carmela Soprano because the
13 government has targeted her husband, Tony, is simply
14 ridiculous. And it shouldn't be that something that's
15 countenanced by this panel.

16 Second, robot searching as searching. The
17 IC's central claim is that human eyes are required
18 before Americans are considered to have their rights
19 impacted by what they're doing. Under both the first
20 and the Fourth Amendment, this position must be
21 rejected, robot searching as searching.

22 Third, judicial reviews of protocols and

1 their implementation is not the same as actual
2 judicial review of individual cases involving people,
3 whether in civil litigation or criminal defense. And
4 aligning those two things, I think, is a mistake and
5 one that you shouldn't replicate. Just because
6 somebody in a black robe is involved doesn't mean that
7 you have judicial review, as enacted in the
8 constitution and law.

9 And fourth, given the massive scale of this
10 surveillance, it is not surprising that it simply
11 cannot be done within the boundaries of even the
12 limited accountability measures that Congress is
13 implicated or that the Agency has positioned for
14 itself. In short, surveilling the whole world or even
15 the portion of the whole world whose internet traffic
16 transits the U.S., it's a hard thing to do. That's
17 the reason that there are multiple pages of compliance
18 incidents that were gathered by our friends at the
19 Brennan Center, and that those things are going to
20 continue. This is -- this scale is too hard to do
21 well and we need to recognize in a way that respects
22 people's human rights and I think it's time that we're

1 honest about that and put on the table, the idea that
2 maybe if something is really this hard, it's not
3 something that we should try to do.

4 MS. FRANKLIN: Okay. Thank you. I'm going
5 to need to ask you to wrap up there, so.

6 MS. COHN: Okay. Well, I tried to stay
7 (cross talk).

8 MS. FRANKLIN: So we have time for questions.
9 Thank you.

10 MS. COHN: Thank you.

11 MS. FRANKLIN: Thank you. Okay. Turning
12 next to Mike Herrington for brief opening remarks,
13 please.

14 MR. HERRINGTON: All right. Thank you. Good
15 afternoon. And thank you, Chair Franklin, and other
16 members of the Board for the opportunity to contribute
17 to this important discussion. As an FBI agent who has
18 investigated cyber national security cases since
19 before FISA Section 702 was created, I've personally
20 used both it and traditional FISA as a case agent in a
21 wide variety of leadership roles. So, I've seen
22 firsthand the value this authority brings to the FBI's

1 mission to protect the American people and uphold the
2 constitution.

3 From the FBI's perspective, the primary
4 national security threats to the homeland now reside
5 outside the United States. We must collect outward to
6 protect ourselves inward. And there's no more agile
7 or efficient tool to do so than 702. This agility is
8 particularly important in a technology environment
9 where foreign threat actors can move to new
10 communication accounts and infrastructure in a matter
11 of hours, if not minutes. Section 702's precision
12 lets us home in on only the information necessary and
13 relevant to investigating and countering foreign
14 threats.

15 To more concretely illustrate its value, let
16 me tell you a few stories about how the FBI uses
17 Section 702 to protect the homeland. In particular,
18 I'd like to focus on the importance of querying
19 Section 702 data for terms related to U.S. persons or
20 USPER queries, a topic which I know has seen a lot of
21 interest recently. While these are hypothetical
22 scenarios, they're closely based on actual cases where

1 we've used FISA 702 and USPER queries to protect
2 Americans from three of our biggest national security
3 threats.

4 First, terrorism. The FBI receives a tip
5 that a foreign terrorist organization is targeting a
6 particular U.S. person. So we regularly query Section
7 702 data for that potential victim's identifiers and
8 in one of those queries, find specific plans to target
9 him through an unwitting associate. Because of those
10 queries, we're able to get both U.S. individual's
11 specific information to protect themselves before the
12 terrorist take action.

13 Second, counterintelligence. The FBI finds a
14 foreign spy possesses identifiers for dozens of U.S.
15 persons. We query those identifiers against Section
16 702 data to determine which of those individuals might
17 be actual or potential victims, in need of defensive
18 briefings or other protective measures and which might
19 be accomplices or co-optees in need of further
20 investigation. The queries allow us to efficiently
21 and selectively review foreign communications to
22 answer that question instead of using other possibly

1 more intrusive, techniques to accomplish the same end.

2 Third, cyber. A U.S. company suffers a
3 breach and the FBI has a reason to believe it maybe
4 the work of a foreign cyber actor. So, we query
5 identifiers related to the company, including
6 employees whose accounts may have been targeted in the
7 incident. In a situation where every passing minute
8 could mean irreparable damage or loss of data, these
9 queries allow us to quickly determine attribution,
10 identify adversary footholds on the network, and share
11 specific information about the cyber group with the
12 company, allowing them to uncover the full extent of
13 the breach and evict the bad actors.

14 So, as you can see from these three examples,
15 querying our lawfully acquired and held FISA
16 information is crucial to finding threat intelligence
17 in a targeted and efficient manner, so we can act on
18 it quickly enough to prevent damage before it happens.
19 Now, many of you may be tracking the FBI's compliance
20 challenges related to us for queries of Section 702
21 data, such as those noted by the Foreign Intelligence
22 Surveillance Court, in its since-declassified November

1 2020 opinion.

2 While it's important to note that the Court
3 did not find unlawful purpose or bad faith, the high
4 rate of non-compliance found by the Court and other
5 oversight bodies over the past couple of years is
6 nevertheless unacceptable. As Director Wray has said
7 publicly, he's "hell bent" on doing whatever it takes
8 to fix our compliance, and that's a feeling all of us
9 in FBI leadership share.

10 So, what have we done about it? After a hard
11 look at the types of errors that we were seeing, the
12 FBI implemented a series of major reforms throughout
13 2021 and 2022 to address their root causes. We made
14 changes to our database systems to enhance
15 understanding and compliance, including switching the
16 default setting, so users must affirmatively choose to
17 have their queries run against FISA data. We
18 instituted pre-approval for certain categories of
19 queries, in some cases requiring the Deputy Director
20 of the FBI to personally approve queries before they
21 are run.

22 We clarified our guidance to the workforce on

1 query standards and created new, improved and
2 mandatory training on those standards. While initial
3 indications from these reforms are promising, we're
4 committed to continuing to take whatever steps we must
5 take to get it right. To that end, I would highlight
6 one more important reform, the creation of a new
7 Office of Internal Audit solely focused on evaluating
8 our FISA compliance and recommending reforms on an
9 ongoing basis.

10 Finally, I want to make sure we don't lose
11 sight of the fact, as we contemplate renewal of this
12 important authority, that we will need it not to
13 counter the threats of the last 5 years, but those of
14 the next 5 years and beyond. As foreign terrorist
15 organizations reconstitute and pose a resurgent threat
16 to the homeland, as foreign cyberattacks continue to
17 escalate in sophistication and frequency, and as we
18 enter into an era of heightened strategic competition,
19 the foreign intelligence we depend on Section 702 to
20 collect will become even more crucial to protecting
21 the United States and its interests. And loss of this
22 vital authority would leave us vulnerable to all of

1 those threats as they grow in intensity over the
2 coming years. Thank you.

3 MS. FRANKILIN: Thank you. We'll next hear
4 from Jeff Kosseff.

5 MR. KOSSEFF: Thank you, Chair Franklin and
6 members of the board. Thank you for the opportunity
7 to discuss Section 702. The views that I expressed
8 today are only mine and don't represent the Naval
9 Academy, Department of Navy, Department of Defense or
10 any other party. So, that said, I first want to
11 express my appreciation for the absolutely crucial
12 work that the Board has done over the past decade in
13 gathering information about 702 and clearly explaining
14 to the public how the program works. Such objective
15 narratives are precisely what we need at this time.

16 So, I began examining 702 in 2015, when my
17 then colleague at the Naval Academy, Chris Inglis,
18 invited me to write a paper with him for a series
19 about 702. I devoted a great deal of time to
20 reviewing public material about how the program
21 operated, including this board's excellent report, as
22 well as the Court opinions that assess the program.

1 In the 2016 paper, Chris and I concluded that
2 702 is constitutional and reasonable under the
3 totality of the circumstances based on what we knew
4 from the public record. Now, the public's knowledge
5 of the facts of the 702 program have evolved since
6 2016. And those facts have challenged me to
7 reconsider whether I personally think that the program
8 is constitutional. While I continue to believe that
9 the program is absolutely essential for national
10 security, and that many of the programs are very well
11 managed to protect privacy, I have very deep concerns
12 about the FBI's access to 702 data and in particular
13 the U.S. person it bear issue.

14 This started with the October 2018 FISA
15 opinion finding, "The government has reported a large
16 number of FBI queries that were not reasonably likely
17 to return foreign intelligence information or evidence
18 of a crime." The Court noted some instances in which
19 FBI employees and contractors queried 702 data for
20 personal reasons. And the Court found that the
21 querying was unreasonable under the Fourth Amendment
22 and came up with a cure involving documentation.

1 Now, I questioned whether those changes fully
2 addressed to those concerns, particularly after the
3 December 2019 Court opinion that found, "Widespread
4 violations of varying standard" by the FBI, including
5 queries about people who visited FBI offices for
6 purposes such as performing maintenance. Then we had
7 the November 2020 opinion released to the public in
8 April of 2021, where the FISA Court found additional
9 problems, including the use of information to screen
10 applicants for the FBI Citizens Academy program.

11 Now, I'm glad to hear today about the 2021
12 and 2022 reforms, but after these three FISA Court
13 opinions in a row that documented compliance failures,
14 I personally, I'm not prepared to believe all of the
15 problems are fixed. I hope that they are, but I think
16 we need far more information and that's where the
17 Board can help. These problems are particularly
18 concerning to me, in light of last year's disclosure
19 by the DNI that the FBI had conducted up to 3.4
20 million U.S. person queries in 2021.

21 Now, that could be overstating the number,
22 but I can just say when I first looked at this program

1 back in 2015, I never would have imagined it was that
2 many U.S. person queries, and I hope the Board will
3 find more -- gather more information on those numbers.
4 Now all of this raises serious questions about the
5 FBI's ability to self-regulate its access to 702 data
6 under the current governance framework. Now, I'm not
7 one for conspiracy theories about surveillance, I've
8 been more than willing than most people to assume that
9 the FBI and other agencies are properly accessing 702
10 data.

11 Nearly 6 years ago, I testified to the House
12 Judiciary Committee that I believed 702 was
13 constitutional and that its national security benefits
14 far outweigh privacy concerns. But at a certain
15 point, we must stop giving the nation's largest law
16 enforcement agency every benefit of the doubt. The
17 FBI cannot play fast and loose with American's most
18 private information, this has to stop now. And if the
19 FBI cannot stop itself, Congress has to stop in --
20 step in.

21 Now, the Fourth Amendment is not our only
22 safeguard against government privacy intrusions.

1 While it provides vital protection, statutes can fill
2 in the gaps if we determine that certain practices are
3 unacceptable. We have the Stored Communications Act
4 and the Wiretap Act. Local governments are
5 restricting law enforcement's use of facial
6 recognition. Given the repeated findings of these
7 compliance problems, Congress should consider imposing
8 more statutory limits on the bureau's ability to query
9 702 data.

10 One option would be to require a warrant for
11 the FBI to query 702 information about U.S. persons.
12 Of course, Congress would need to consider the trade-
13 offs in imposing such a requirement. The DNI states
14 that a warrant requirement would -- could hamper the
15 speed and efficiency of operations and I don't
16 trivialize those needs.

17 I'm sure there are many cases in which easier
18 querying of 702 data would benefit national security.
19 But the question for Congress is not whether
20 warrantless government querying would have some
21 benefits, because of course they would, but whether
22 those benefits outweigh the privacy intrusions of the

1 warrantless queries. And I don't pretend to have an
2 answer to this difficult policy question, particularly
3 because the amount of public information that we have
4 about 702's operation is limited, with the most
5 valuable data scattered across redacted Court opinions
6 that are publicly released months after they're
7 written. So, as you prepare your next report, I hope
8 that you can help to provide a more complete picture
9 of how the FBI query 702 data and the benefits that
10 702 provides.

11 Now, I want to conclude by saying, I don't
12 want my criticism of this aspect of 702 to be seen as
13 a call to allow 702 to expire. 702 is absolutely
14 vital to national security, and we must preserve it.
15 But we must do so in a way that protects our
16 fundamental civil liberties. Thanks for inviting me
17 to speak. And I look forward to your questions.

18 MS. FRANKILIN: Thank you. And the final
19 panelist to offer a brief opening remark will be
20 Jonathan Mayer.

21 MR. MAYER: Thank you. Thank you, Chair
22 Franklin, and members of the Privacy and Civil

1 Liberties Oversight Board for convening this important
2 and timely public forum on Section 702. Section 702
3 is among the most effective and most contested
4 surveillance authorities available to the U.S.
5 intelligence community and PCLOB is playing a central
6 role as Congress considers reauthorization this year.
7 I offer that view from firsthand experience.

8 Before joining the Princeton faculty, I
9 served as a staff member in the Senate, where I worked
10 on the Intelligence Committee and Judiciary Committee
11 bills that culminated in the FISA Amendments
12 Reauthorization Act of 2017. That legislation
13 implemented modest reforms and set the current sunset
14 date of December 31, 2023. That most recent
15 reauthorization process was difficult for members and
16 staff. Foreign Intelligence Surveillance is a complex
17 area of statutory and constitutional law, and IC
18 practices are both technically sophisticated and often
19 classified.

20 As an example, there was a legislative staff
21 briefing on Section 702 in the weeks before
22 reauthorization. We were about 30 minutes in and had

1 reached the Q&A section. A senior legislative staff
2 member in the senator -- in senator's office who is
3 responsible for advising the members vote on
4 reauthorization, raised their hand and earnestly
5 asked, what's Section 702. So, you have your work cut
6 out for you. I commend the board and staff for taking
7 a fresh look at Section 702 in this year's
8 reauthorization cycle, and for aiming to release the
9 report in the spring.

10 Should that target date for a formal report
11 slip, I would strongly encourage you to provide
12 whatever substantive input to Congress that you can in
13 the coming months. In the last reauthorization cycle,
14 committee bills form the framework for reauthorization
15 policy debates. Once those base bills were developed,
16 it was difficult to make changes. So, I want to
17 emphasize in the clearest possible terms that for
18 PCLOB to best serve Congress and the American people,
19 you must move quickly.

20 In the balance of my opening statement, I'd
21 like to emphasize a foundational issue for Section
22 702. How does the surveillance authority affect

1 ordinary Americans? When the IC conducts Section 702
2 surveillance, it incidentally collects communications
3 to or from people in the United States and U.S.
4 persons abroad. These are persons who are not targets
5 of Section 702 surveillance, who could not lawfully be
6 targets of Section 702 surveillance and were otherwise
7 protected by a warrant requirement under FISA and for
8 persons in the United States under the Fourth
9 Amendment of the Constitution.

10 Current law allows the IC to query this
11 incidentally collected data with the U.S. person
12 identifiers for foreign intelligence and law
13 enforcement purposes. For 15 years, members of
14 Congress on both sides of the aisle and civil society
15 groups from across the political spectrum have
16 repeatedly called on the IC to quantitatively estimate
17 the extent of Section 702 incidental collection.
18 Section 702 also includes a conditional requirement
19 for the IC to estimate incidental collection.

20 The IC for its part has closely considered
21 this issue and has not identified an estimation method
22 that it finds feasible. As the board wrote in its

1 2014 report on Section 702, the volume of incidental
2 collection is one of the biggest open questions about
3 the program and a continuing source of public concern.
4 The unknown and potentially large scope of the
5 incidental collection of U.S. persons communications,
6 the Board explained, pushes the program close to the
7 line of constitutional reasonableness. But because of
8 the impasse over estimation methods, lawmakers and the
9 public do not have even a rough estimate of how many
10 communications of U.S. persons are required under
11 Section 702.

12 I'm here today because I believe there is a
13 possible path forward to resolving that impasse. When
14 I served in the Senate, the DNI noted in a public
15 hearing that the IC would welcome outside technical
16 assistance about how to estimate incidental
17 collection. My research group at Princeton took up
18 the challenge broadly engaging with experts,
19 stakeholders from government, industry and civil
20 society. We spent several years developing a new
21 estimation method. And we published our primary
22 research article this past August.

1 The project is, to our knowledge, both the
2 only peer reviewed scientific proposal for estimating
3 incident collection and the only detailed alternative
4 to the sampling and manual analysis methods that the
5 IC has consistently declined. I want to specifically
6 acknowledge my co-author (inaudible) and -- well, the
7 views I offer at this public forum are solely my own,
8 the research that I'm describing here is very much a
9 collaborative effort.

10 The key idea in our proposal is that
11 communication services such as webmail providers and
12 telephone carriers maintain highly accurate country
13 level location data in the ordinary course of
14 business. The IC could match its own dataset about
15 Section 702 collection with these external location
16 datasets, and compute aggregate estimates of
17 incidental collection. Let me briefly touch on why,
18 as I understand the IC's experience, estimating
19 incidental collection is so difficult. An estimation
20 method must protect intelligence sources and methods
21 and must respect privacy and civil liberties. It must
22 comply with the law. It must impose a limited burden

1 on IC capacity. It must rely on high quality data.
2 It must be transparent and repeatable. It must use
3 cryptography standards approved by the IC. It must
4 account for differences in data formatting. And it
5 must account for change over time. I elaborate on
6 each of these requirements in my prepared statement.

7 And in short, I believe that our proposal for
8 estimating incidental collection under Section 702
9 appears to satisfy each and every one of these
10 criteria. While I'm heartened by the earnest response
11 we've received, I also fully acknowledge that taking
12 steps forward will not be easy.

13 And so, in closing, I'd like to suggest that
14 as the Board moves forward with Section 702 oversight,
15 I encourage you to consider assessing how the IC is
16 implemented and could implement the statutory
17 provision that conditionally requires an estimate of
18 incidental collection. Thank you again for convening
19 this public forum. And I look forward to your
20 questions.

21 MS. FRANKLIN: Thank you. Okay. So, we're
22 going to reverse the order of the Board members and

1 questions. So, we'll turn first to Rich DiZinno.

2 MR. DiZINNO: Thank you, Chair Franklin. And
3 this question is directed to Mr. Herrington. There's
4 been a lot of discussion in this forum and outside of
5 this forum about the compliance issues that FBI has
6 faced with respect to U.S. person queries. These
7 compliance issues are very concerning, especially with
8 respect to the implication for and the impact on the
9 privacy and civil liberties of U.S. citizens. You
10 mentioned some of the changes that the FBI has made to
11 improve privacy and security in your opening
12 statement.

13 Can you go into a little bit more detail
14 regarding the reforms that had been made? And in
15 particular, can you explain how we, how Congress, how
16 the American people can be reassured that these
17 significant compliance issues will be, if not
18 eliminated, then at least drastically reduced? And
19 then separately, I'd like you to address, please, the
20 impact of additional restrictions on U.S. person
21 queries in the form of a warrant requirement?
22 Meaning, what impact would that have as a process

1 matter and what impact that would have as an
2 operational matter, in terms of the FBI's ability to
3 do the kinds of things that you described in your
4 opening statement?

5 MR. HERRINGTON: All right. Thank you,
6 Member DiZinno, for that question. So, it's a lot of
7 important issues and I do think it's worth exploring
8 this issue further than I was able to in my initial
9 remarks. First, let me run down through some more
10 specifics on the reforms that we've implemented.
11 First, you know, we identified several areas where our
12 databases were, you know, not configured in the most
13 advantageous way. And in particular, the one that I
14 noted where we've changed the default, so that in some
15 of our databases that are running against multiple
16 datasets, a user with access to FISA data will no
17 longer have to unselect when they run a query, that it
18 will run against FISA data. In fact, they have to
19 affirmatively select, and in doing so, you know, think
20 about whether that query meets the query standard.

21 So that is one thing that resulted in a lot
22 of queries that we had had that may have not been

1 intentionally run against FISA data. And in some --
2 in many cases, those still met the justification
3 standard, regarding the query standard, but in many
4 cases they did not. And so that resulted in issues of
5 non-compliance. We've also identified two specific
6 areas where we need pre-approval for queries. One is
7 batch queries in 100 or greater terms in one single
8 query. And another is querying, you know, sensitive
9 terms such as those related to, you know, an elected
10 official or a journalist or a member of the press.

11 In the first case, an attorney must approve
12 that. And that's because just due to the number of
13 terms that are implicated in a batch query. If that
14 justification was not met, then it would have a
15 greater privacy impact. In the second case, I think
16 it's obvious, you know, why we would need preapproval
17 for targets that are for terms that are related to
18 people in particularly sensitive situations,
19 including, you know, some of the concerns about
20 politicization of intelligence tools.

21 And then the last is one thing that we found
22 is that a lot of the compliance incidents related to

1 failing to meet the query standard were due to a lack
2 of understanding of what that query standard was, and
3 in fact, you know, due to lack of clarification or
4 communication of that. So, as I said, we clarified
5 that to make sure that it is clear that we are not to
6 be using it in some of the vetting incidents that were
7 cited, you know, in an earlier statement, and unless
8 they affirmatively meet the reasonably likely to
9 retrieve foreign intelligence information or evidence
10 or a crime standard.

11 And also we have included very concrete
12 examples in that training so that we can better convey
13 that standard to our workforce, and we've also made it
14 a mandatory annual requirement to retain access to the
15 database. So, I would note that, you know, the
16 compliance incidents that have been made public to
17 this date predate all of those changes. So, I would
18 say it is important to, once we start making public
19 the result of oversight that postdate those, that we
20 compare and view the results of those changes, which
21 as I said, are promising, you know, from our
22 perspective, although defer to DOJ and ODNI to provide

1 more detail on that point.

2 Finally, on the impact of a warrant
3 requirement. That would depend greatly on the legal
4 standard applied. I'm assuming, based on the
5 discussion here, that what we're talking about is a
6 probable cause standard. Now, you know, I'm not a
7 lawyer, but I know the FISC has repeatedly held that
8 querying data that is lawfully collected and held by
9 the government is not a Fourth Amendment search,
10 although I've heard various views regarding that in
11 the discussion here. But I want to focus more on an
12 operational impact. And I see two major impacts. One
13 is that the process would become so burdensome, that
14 it would really be tantamount to a de facto ban on
15 querying USPER terms against this dataset. And the
16 second one is that it would really prevent us from
17 connecting the dots, and would in fact go towards
18 rebuilding the wall that the 9/11 and Fort Hood
19 Commissions identified in their studies that prevent
20 the effective connecting of the dots and sharing
21 information among agencies.

22 So, to understand the first point, I'd like

1 to consider the hypotheticals from my remarks. First,
2 you know, in many cases, we can't wait the weeks or
3 months for the results that would be required to
4 actually seek an order from the FISC. And that could
5 prevent us from, for example, mitigating an ongoing
6 cyber intrusion or preventing a terrorist attack
7 before it happens or could even delay valuable
8 defensive briefings that we're giving to somebody who
9 is being targeted by a foreign spy.

10 Also, there are some cases, in lot of cases,
11 important cases, we wouldn't really have enough
12 information to meet a probable cause standard. Think
13 about those hypotheticals which represent actual,
14 important use cases. The fact pattern in a lot of
15 them doesn't support a probable cause finding on those
16 specific terms, that would nevertheless be valuable in
17 those situations in part because many of them pertain
18 to actual or potential victims. And also another
19 important point there, if we do have probable cause
20 for a particular USPER term or individual, we would
21 likely be well beyond the point in the investigation
22 where a query would even be valuable or useful. And

1 instead, we would likely seek a warrant to conduct an
2 actual Fourth Amendment search on the relevant person,
3 account, or et cetera.

4 At the end of the day, we receive tips about
5 threats and have a responsibility to follow-up on
6 them. Our agents and analysts have a discretion about
7 how they use their time and in doing so and how they
8 can best use their time. So, you know, using -- given
9 -- putting -- imposing this onerous requirement would
10 mean that many more of them would just resort to
11 manual review of the data, instead of seeking an order
12 for a query which they are permitted to do. They can
13 manually review line by line everything in this data.
14 That would be more resource intensive to be sure,
15 which I understand is not a compelling argument to
16 many. But any -- the fact remains that, you know, any
17 agent analyst who is reviewing 702 data line by line
18 is not doing other things to protect Americans. But
19 more importantly, that could have the opposite effect
20 on privacy than is intended by emplacing this
21 requirement.

22 Manual review, line by line would be less

1 targeted and selective in reviewing that data. And
2 also, we might have to use other investigative
3 techniques, instead of querying, which might be more
4 intrusive, to answer a question that simple query of
5 702 data may have been able to answer without going
6 into that more intrusive technique.

7 MS. FRANKLIN: Thank you. I'm sorry. We do
8 want to get to other board member questions. Just --
9 it's a very, very important topic, but I do thank you.

10 MR. HERRINGTON: Yes. Thank you.

11 MS. FRANKLIN: I'm turning to Ed Felten.

12 MR. FELTEN: Thanks. My question is also for
13 Mr. Herrington. In your testimony, you gave several
14 examples of querying -- how querying 702 data helped
15 the FBI protect Americans from foreign threat actors.
16 And I couldn't help but notice that in each of your
17 examples, the FBI was querying for U.S. person as a
18 victim or potential victim of a foreign bad actor,
19 rather than querying U.S. persons as potential
20 perpetrators of crime.

21 So, in light of your examples, is it fair to
22 say that a primary use or primary value for the FBI

1 mission of Section 702 of U.S. Person queries comes
2 from searches related to potential U.S. victims,
3 rather than perpetrators? And what statutory or
4 procedural safeguards exist to protect the privacy of
5 U.S. persons in this scenario of a search of that U.S.
6 person as a potential victim?

7 MR. HERRINGTON: Thank you, Member Felten,
8 for that question. So, I did focus my scenarios
9 which, again, are hypothetical scenarios, but based
10 on, you know, actual facts of cases on that because I
11 do think that that is one area that is a very
12 important use of this tool, and one that's
13 particularly important for the FBI in our mission to
14 protect Americans and, you know, notify and warn and
15 protect victims. I -- I'm not sure the word primary
16 would apply there because I don't have statistics as
17 to what proportion of our queries actually apply to
18 actual or potential victims, rather than, you know,
19 actual or potential subjects of an investigation.
20 However, it is very -- it is a very substantial and
21 important purpose for this.

22 And in terms of protections for U.S. persons

1 whose terms may be queried as actual or potential
2 victims. You know, there are several layers of civil
3 liberties protections baked into FISA and into Section
4 702. In particular, you know, in our minimization
5 procedures, our querying procedures, our targeting
6 procedures, and at the end of the day, any of these
7 queries has to meet the query standard, which is
8 reasonably likely to retrieve foreign intelligence
9 information or evidence of a crime.

10 MS. FRANKLIN: Thank you. All right. So, I
11 get the next question and I'm going to turn to Cindy
12 Cohn, please. So, you spoke a little bit about some
13 of the longstanding lawsuits that EFF has brought and
14 the barriers you face during the state secrets
15 privilege. And one of those, as I understand it, the
16 underlying claim that you have been seeking to
17 litigate, but have not been able to litigate involves
18 upstream collection under Section 702 and how EFF
19 challenges under -- under the Fourth Amendment, that
20 this would violate the Fourth Amendment and raise
21 certain privacy issues. Could you speak to both the -
22 - the legal claim, but also just from a privacy

1 interests perspective, what risks EFF sees with
2 upstream, even with Abouts Collection suspended?
3 You're on mute. You're on mute.

4 MS. COHN: Wouldn't be a meeting if I wasn't
5 on mute. Hi. The EFF believes that all people,
6 including Americans, have the right to have a private
7 conversation in the digital age and that it should not
8 be subjected to review, even robot or momentary review
9 by law enforcement without meeting some standard and -
10 - and the intelligence community. I mean, I think
11 that we have to center what we're trying to protect
12 here, which is the ability to have a private
13 conversation and the ability to associate with others
14 without governmental review in the first instance. I
15 think that's what, you know, Mr. Sanchez was talking
16 about when he was talking about general warrants and
17 writs of assistance, but the Fourth Amendment as a
18 whole. I also think that's embedded in our basic
19 privacy law, whether that's the Wiretap Act or
20 otherwise.

21 So, the risk is that the human right to be
22 able to have a private conversation or privately

1 associate is something that we all should enjoy, and
2 that it has gone away. Secondary risks include the
3 kinds of things that we've been talking about, about
4 the, you know, the ongoing difficulty of the
5 intelligence community in the FBI specifically to
6 actually even do what they said they were going to be
7 able to do in a very limited way. The worst case
8 scenario is a criminal prosecution of someone that's
9 based upon evidence that they cannot interrogate,
10 which we have seen, you know, courts refuse to really
11 pay attention to, but I think is a serious problem.
12 And the fact that we have on paper, the idea that you
13 should be able to confront your accusers and the
14 evidence arrayed against you, but we have several
15 cases now where that has not actually existed, that we
16 know about, and I suspect untold others that we don't,
17 given some of the techniques that have been uncovered
18 about how law enforcement and national security will
19 hide the use of intelligence collected information for
20 prosecutions. I think that's the worst case scenario
21 is that people are going to jail without being able to
22 confront their accusers and the evidence against them.

1 As I mentioned, and I've said a couple of
2 times, I think there's also First Amendment
3 implications here. We talk a lot about the Fourth
4 Amendment, and those are important. But we also have
5 a right to associate in this country without being
6 tracked and without our associations being tracked.
7 And that's another issue that EFF has tried to bring
8 up in litigation and has ended up stymied, but a --
9 but stymied for reasons that don't have to do with the
10 merits of the claim. And I think it's important for
11 us as a society to recognize that the kinds of contact
12 tracing tools and other things that are being deployed
13 and used against U.S. persons have implications for
14 the ability to people to associate as well as for --
15 for the -- the basic privacy rights.

16 MS. FRANKLIN: Thank you. Over now to Beth
17 Williams.

18 MS. WILLIAMS: All right. So, this question
19 is for Mr. Herrington, and thank you to all of our
20 panelists for being here. You know, you mentioned the
21 wall, Mr. Herrington, and that's actually what I was
22 hoping you could talk a little bit more about, because

1 after September 11th, both the 9/11 Commission, and
2 the Inspector General at the Department of Justice
3 concluded that the wall that had been erected between
4 national security intelligence investigations and
5 criminal cases prevented the sharing of information
6 that two of the terrorist hijackers were in the United
7 States. And as a result, many of the reforms after
8 9/11 were geared toward more information sharing among
9 the intelligence community.

10 You talked a little bit about your concerns
11 about this. Can you talk -- can you explain why
12 you're concerned about why certain changes to Section
13 702 might be rebuilding this wall? And, you know, if
14 those are concerns, is there another way to solve some
15 of the FBI's compliance problems in order to better
16 protect privacy and civil liberties without rebuilding
17 those -- those bureaucratic hoops that prevented us
18 from stopping September 11th?

19 MR. HERRINGTON: All right. Thank you,
20 Member Williams. It's a great question. I appreciate
21 the -- the opportunity to respond to that. So, I
22 would say, it's important to note here that, you know,

1 we have already kind of self-imposed, and for good
2 reason, some restrictions on our sharing of
3 information between agencies as it pertains to the
4 Section 702 program specifically. And that is that --
5 the FBI only receives a relatively small portion of
6 the total 702 collection, I believe it was about 4.4
7 percent in last year's ASTR that was reported,
8 because we limit our access to that collection to only
9 those targets that are relevant to a full predicated
10 national security investigation, so that we can use
11 this in a more targeted manner to fulfill our mission,
12 which is to protect the Americans or to protect
13 Americans and uphold the Constitution.

14 So, just referring back to my hypotheticals,
15 I think that's the best way to illustrate the danger
16 of, for example, a warrant requirement, and how that
17 might constitute rebuilding the wall. So, in the
18 first one, like, if a terrorist organization were
19 targeting a particular individual, what if the team
20 who's reviewing that manually, because they don't have
21 the ability to query that, does not know that a
22 subject who is monitored by another field office is

1 involved in that and that other subject has key
2 information that would help prevent the -- the threat.
3 They would not find that in their manual review of
4 their own select targets that they know to review.

5 Also in the cyber example, what if we thought
6 it were one particular cyber group that may have done
7 this based on our best guess, but it actually turned
8 out there was another one. And because we didn't
9 query our holdings writ large, we didn't find that
10 information and we're unable to establish attribution.
11 It would be pretty much infeasible to review the
12 totality of our cyber related investigation every time
13 that there's a cyber incident, even if you're only
14 considering those that do meet the query
15 justification. So, those are some of the concerns
16 that we have as constitutes rebuilding the wall.

17 Now, in terms of what we might accept short
18 of a warrant requirement. I'm not really in a
19 position to get to specific proposals today, but I
20 would echo General Nakasone's remarks by saying that
21 FBI is committed to keeping Section 702 a tool that
22 preserves and protects both national security and

1 civil liberties and privacy. And we look forward over
2 the coming months to discuss potential reforms that
3 allow us to do both even better.

4 That being said, I do have a few points to
5 make on the topic. First, as I discussed, we've
6 already implemented significant reforms to our USPER
7 query compliance. And we did that by looking at the
8 areas where the FISC and other external oversight
9 bodies found that we fell short, allowing us to
10 identify the root causes and tailor those reforms
11 specifically to directly address those causes. So, I
12 think there's a few important criteria that we keep --
13 should keep in mind when evaluating proposals for
14 reforms. The first pertains to that point, is the
15 proposal reform based on analysis of actual
16 shortcomings in the authority and is - is it
17 specifically tailored to fix the root causes. The
18 second, and as we've emphasized in the run up to prior
19 reauthorizations, it's important this authority --
20 authority remain technology neutral to avoid being
21 made obsolete by new advancements in technology. So,
22 does the proposal reform preserve the authority's

1 technological neutrality? And third, does the
2 proposed reform preserve the efficacy of this
3 important authority? And does it curtail that
4 efficiency in significant ways?

5 So, those are some of the questions that we
6 would consider when we're looking at proposed reforms.
7 And we'd certainly be more inclined to support
8 proposals that meet those three criteria. They're
9 guided by analysis of where specifically improvements
10 are needed. They keep Section 702 technology neutral,
11 and they preserve the efficacy of this vital
12 authority.

13 MS. FRANKLIN: Thank you. Over to Travis
14 LeBlanc.

15 MR. LeBLANC: I have a question for Professor
16 Mayer. Thank you for joining us today and providing
17 your analysis and proposal on the incidental
18 collection of U.S. person information. You're not
19 only an accomplished academic, but you also have
20 critical experience working in the U.S. Senate,
21 particularly during the last reauthorization. With an
22 eye towards your legislative experience, do you

1 recommend that Congress clarify its legislation and/or
2 mandate NSA provide an approximate count of U.S.
3 person information? And additionally, do you have
4 other recommendations for 702 reforms that you would
5 encourage the board to propose in its updated Section
6 702 report?

7 MR. MAYER: Well, thank you for the question,
8 Board member LeBlanc. I think before getting to the
9 issue of whether statutory changes are needed, with
10 respect to estimating incidental collection, I think
11 it's worth trying without statutory changes. In our
12 analysis of the applicable law for the proposal we
13 have developed, we do not see at this stage legal
14 barriers to implementing the proposal. Those may
15 arise. There may be other barriers that arise. And
16 if that's the case, I would also like to see Congress
17 move on that issue in advance of reauthorization. And
18 I think it would be unfortunate to have another cycle
19 of reauthorization where we don't have access to this
20 important information. So, that would be my hope with
21 respect to estimating incidental collection.

22 You asked about other aspects of the

1 reauthorization. And without going into any
2 deliberations from the -- confidential deliberations
3 from the last reauthorization, I would call the
4 board's attention to two provisions that have already
5 come up. One about Abouts Collection and the other
6 about U.S. person queries. There was discussion in
7 the prior panel about the Abouts Collection provision
8 that Congress added to Section 702 in the most recent
9 reauthorization. And the discussion about that
10 provision was largely; one, about legislative
11 procedure. Under the current provision, Congress gets
12 notice about the upcoming resumption of Abouts
13 Collection, and then it's up to Congress what to do
14 about it.

15 And so in essence what that provision does is
16 it flips the default for how Congress might act on
17 Abouts collection. Instead of Congress having to
18 affirmatively authorize about this collection, you
19 know, the President then signing that bill. In this
20 case, Congress gets noticed, and then it's up to
21 Congress if it wants to essentially opt out of that
22 new form of Abouts Collection. And it's difficult to

1 see that happening on any quick timeline. And, of
2 course, this is presupposing that the intelligence
3 community has decided to do this and that intelligence
4 community reports to the President. And so we're not
5 talking about a situation which not only Congress
6 would have to pass legislation, declining to allow
7 that Abouts Collection, but actually have to override
8 a veto. So I think that it is difficult to see that
9 provision having much substantive impact. And my
10 recommendation for consideration there would be to
11 just flip the default back the other way. So, if the
12 intelligence community has a proposal for resuming the
13 Abouts Collection, there was nothing stopping the
14 intelligence community from approaching Congress with
15 that proposal and seeking legislation to authorize
16 that proposal.

17 The other provision, and the last provision I
18 want to touch on is around US person queries. Again,
19 this has come up already today. This is the provision
20 702 F2, which provided for judicial review of results
21 of certain FBI U.S. person queries. That part of FISA
22 was introduced as a compromise, as an alternative to a

1 requirement for a warrant to conduct U.S. person
2 queries or to review the results of U.S. person
3 queries. And there was pervasive confusion at the
4 time about the difference between the warrant proposal
5 and this proposal.

6 And I just want to close by emphasizing how
7 narrow this provision is in ways that I think were --
8 it is fair to say were not evident to many members of
9 the congressional staff at the time. First, this only
10 applies to queries that are not designed to find and
11 extract foreign intelligence information. It is often
12 the case that there is some foreign intelligence
13 component to U.S. person queries. And second, the
14 query has to be performed in connection with a
15 predicated criminal investigation. That is a
16 particular stage in a criminal investigation. There
17 are other types of queries potentially by the FBI that
18 would not be predicated criminal investigation.

19 And then last, that investigation has to not
20 relate to national security. And it's almost a little
21 bit tautological to find a query in Section 702 data
22 where there isn't something touching on national

1 security there. And so, again, there's a lot of
2 confusion among staff about these limiting principles.
3 And I think the Board could do a tremendous service in
4 helping Congress and the public understand those
5 principles. Thank you.

6 MS. FRANKLIN: Thank you. Okay. We're going
7 to turn back to the top of the order and I'm going to
8 ask my fellow Board members, if we can try to keep our
9 questions concise and our panelists also to please
10 keep answers concise, hopefully, we can make it
11 through the order again. Back to Richard DiZinno.

12 MR. DiZINNO: Thank you, Chair Franklin.
13 Back to you, Mr. Herrington. You mentioned in your
14 opening statement having experience using,
15 "Traditional FISA as well as using (inaudible)
16 authority as a case agent." In terms of compliance
17 and abuses, we have seen and there has been reference
18 in this form to the Crossfire Hurricane investigation
19 and the DOJ IG report relating to that, those issues
20 that were brought up.

21 Can you just talk briefly about and describe
22 the differences between Title 1 and the abuses in the

1 context of Crossfire Hurricane and Title 1/traditional
2 FISA versus Section 702, including very briefly the
3 broad purpose and the difference in purpose of each
4 authority and some of the privacy and civil liberties
5 issues that each authority implicates?

6 MR. HERRINGTON: Yes, thank you, Member
7 DiZinno. You know, I would say that they're both very
8 important authorities, but are targeted at very
9 different things. I don't want to get too deep into
10 the Crossfire Hurricane case, or the OIG report on
11 that other than to say that we fully accepted their
12 recommendations and have, you know, implemented
13 several reforms based on and responsive to those
14 investigations or those recommendations.

15 So, Title 1, FISA is, you know, meant to
16 target specifically agents of a foreign power. And so
17 -- and it also has a heavy probable cause requirement
18 to it, as many of you are aware. And that results in
19 a rather long process, particularly when you're
20 talking about situations as in my experience in cyber
21 ones where you are dealing with how to implement
22 collection using a, you know, technologically

1 sophisticated actors who may -- and also actors who
2 may be moving from account to account very quickly,
3 faster than that we can apply for a FISA Title 1, in
4 some cases.

5 So, it's a very limited tool in many
6 respects, that 702 provides a great deal more agility
7 and efficiency in targeting those foreign actors who
8 may be, you know, moving more quickly, and therefore,
9 or using many more, you know, using many more
10 accounts. So, it's just a much more efficient and
11 quicker way to do -- to look into those activities,
12 and answer questions that we have about, you know,
13 threats that we're seeing, you know, in a much more
14 quick manner and do, you know, although we definitely
15 use FISA Title 1 to obtain, you know, information that
16 allows us to prevent attacks, just the agility of 702
17 is valuable in doing that in an even more agile
18 manner.

19 You know, one thing that I would say about
20 the...the... circling back to the Crossfire Hurricane is
21 that, you know, we are required to provide information
22 to support, a lot of inculpatory information and one

1 of the failures, there was a failure to include more
2 exculpatory or information that was casting doubt on
3 those findings. And so we've implemented changes to
4 make sure that we are including that information in
5 the future.

6 MS. FRANKLIN: Thank you. Now to Ed Felten.

7 MR. FELTEN: Thanks. I have a question for
8 Professor Mayer. First, I want to thank you for your
9 work, for your research on methods for estimating the
10 prevalence of U.S. person information in Section 702
11 collection. I think it's important to move the debate
12 forward on that issue. And also mindful of your
13 suggestion that there are things that might be done in
14 advance of the reauthorization deadline to provide
15 useful information for Congress on this question.

16 But I want to ask sort of more generally
17 about this question of estimating U.S. person
18 information. And it seems to me that on this topic,
19 we often let the perfect be the enemy of the good.
20 That is we -- we often and I think sometimes agencies
21 will set a very high bar in terms of the precision of
22 what they're asking for or in terms of minimizing or

1 requiring absolutely zero encounter of U.S. person
2 information in the process.

3 So, I guess, I'd like to ask your opinion
4 about this, in particular, you know, are there simple
5 statistical estimation methods involving, which you
6 mentioned, involving manual evaluation of a small
7 sample that would be viable for agencies. And number
8 one -- and number two, to the extent that U.S. person
9 information is indeed very rare in the collected data,
10 isn't it the case that examining a small sample should
11 encounter little or no U.S. person information?

12 And then finally, to the extent that there's
13 concern about the analysts encountering U.S. person in
14 this information, in the process of an estimation, are
15 there things that could be done by Congress or others
16 to clarify that -- that in the big picture there, it's
17 extremely valuable to understand how -- what the
18 impact is already on U.S. persons and how we could
19 minimize that? So, in general, I'd like your opinion
20 about sort of how to move forward and how we can avoid
21 making the perfect the enemy of the good in this
22 space.

1 MR. MAYER: Well, thank you for the question,
2 the multi-part question, Board Member Felten. Before
3 getting to that, it occurs to me, I didn't quite give
4 a fulsome answer to Board Member LeBlanc on the 702 F2
5 provision. And I just wanted to close that out by
6 noting that I would encourage the Board to consider
7 the limitations on 702 F2. And given that they're so
8 significant right now, potentially consider
9 recommending revising those limitations on 702 F2
10 orders.

11 With respect to the estimation issue, there
12 are a couple of straightforward methodological
13 directions. One would be for agencies within the
14 intelligence community to attempt estimates based on
15 the data that they hold and based on data that they
16 could obtain, whether through web searches or
17 commercial data providers. Another possible approach
18 would be for companies that receive Section 702 orders
19 to attempt estimates based on the orders that they --
20 as to the directives that they've received.

21 Those methods may well be viable. There has
22 clearly been a difference of opinion between the

1 intelligence community and stakeholders, including
2 members of Congress on both sides of the aisle who
3 have advocated for those types of estimation methods.
4 My own view is that there is a potentially viable path
5 forward there in that the privacy implications, while
6 not insignificant, could be managed through procedures
7 developed by the intelligence community, perhaps with
8 input from PCLOB and Congress. But I recognize that
9 there is a reasonable difference of opinion about
10 those particular directions.

11 And I would say, the data access issue here
12 is just as significant as the privacy issues. If
13 you're going to estimate incidental collection, you
14 need to be able to match up information about Section
15 702 collection with where people are located or their
16 nationality. And that's not easy data to come by.
17 And there are some real questions about the commercial
18 data in this space. And so in thinking through the
19 viability of the more straightforward methods, I would
20 encourage the Board to think about that data access
21 issue alongside the privacy implications.

22 With respect to what the privacy implications

1 for Americans are, I think it's very difficult to
2 estimate. It may well be that it's a relatively small
3 amount of a sample. And -- and so that would, you
4 know, certainly mitigate privacy concerns around these
5 approaches. But we know that we don't know. So, I'm
6 afraid I sort of can't give more of an answer than
7 that. And that's for managing the privacy impact. As
8 I mentioned, you could imagine very carefully drawing
9 intelligence community procedures around how that
10 analysis is done, how the data is used. Same for any
11 other stakeholders involved in the process and PCLOB
12 and Congress could be involved there.

13 So, again, on balance, I think there may well
14 be a path forward there. But I take it face value,
15 the IC's reluctance, and they've been very consistent
16 in that reluctance.

17 MS. FRANKLIN: Thank you. Back to me. I'm
18 going to ask the last question because we're almost at
19 the end. But I want to make sure to ask the question
20 to Professor Kosseff, thank you for joining us and for
21 your patience as we cycled through the other
22 panelists. But I wanted to ask you, you argued that

1 the significant number of compliance incidents with
2 FBI and the U.S. person queries shows that Congress
3 should consider imposing statutory limits on the FBI's
4 ability to query Section 702 data. Can you elaborate
5 at all on what changes you would recommend for
6 Congress?

7 MR. KOSSEFF: Well, I think part of that
8 really depends on what you find. I'm fairly open. I
9 think, between the compliance incidents and the
10 number, the up to 3.4 million is what's really stuck
11 with me, that is not something I ever would have
12 imagined years ago. But I think probably the -- it
13 could range from a warrant requirement for queries to,
14 I think, also looking at limiting the purposes for
15 U.S. person queries, and saying you can't do it for
16 criminal investigations. I mean, I think, or there
17 can be disclosure requirements or additional
18 procedural requirements.

19 My concern about procedural requirements is
20 that we've imposed some, both sort of administratively
21 and legislatively, and they're not working very well,
22 at least from what we know. So, I feel like we need

1 to figure out something that will make -- will stop
2 this mission creep, frankly.

3 MS. FRANKLIN: Okay. Well, thank you. Thank
4 you so much. And I want to, again, we are at time, I
5 want to thank all of our panelists for participating
6 today, for sharing your thoughts, for sharing a
7 written opening statement with us, which I believe we
8 will be able to post on our website.

9 Also for those watching, we will have this
10 available. The recording will be available on our
11 website. So, hopefully additional folks will be able
12 to watch at that time. And thank you again to
13 everybody. This will be very valuable to us as we
14 continue to move forward with our review and
15 preparation of the Board's upcoming Section 702 report
16 to inform the debate over reauthorization.

17

18

19

20

21

22

1

2

3

4